



ShadowControl CMD User Guide

StorageCraft Copyright Declaration

StorageCraft ImageManager, StorageCraft ShadowProtect, StorageCraft Cloud, and StorageCraft Cloud Services, together with any associated logos, are trademarks of StorageCraft Technology Corporation in the United States and elsewhere. All other brands and product names are or may be trademarks or registered trademarks of their respective owners.

Table of Content

Table of Content	2
1 CMD Overview	3
1.1 CMD in Operation	4
2 Installing CMD	11
2.1 Installing the CMD Appliance	11
2.2 Installing the CMD Agent	12
3 Understanding the CMD Console	16
3.1 Navigation Panel	17
3.2 Main Panel	28
3.3 Session Panel	37
4 Using Status Rule Policies	38
4.1 ShadowControl Rules	39
4.2 ShadowProtect Rules	39
4.3 ImageManager Status Rules	40
4.4 Status Rules Details	40
5 Reporting	42
5.1 Report Scheduling	42
5.2 Sample Report	44
5.3 ShadowProtect Licensing	45
6 Upgrading CMD	46
7 CMD Backup and Restore	47
8 Appendix: Using the CMD Portal	48
8.1 Understanding the Portal Console	48
8.2 Using Org Groups	51
8.3 Portal Report Scheduling	51
8.4 Defining Portal Accounts and Settings	52
9 Appendix: Experimental Report API	53

ShadowControl CMD User Guide

Welcome to the StorageCraft® *ShadowControl™ CMD User Guide*. This Guide describes the CMD monitoring technology, how to use the product, and how to derive maximum benefit from CMD.

This guide covers ShadowControl CMD v2.0.1.

This user guide includes the following major sections:

- [CMD Overview](#)
- [Installing CMD](#)
- [Understanding the CMD Console](#)
- [Using Status Rule Policies](#)
- [Reporting](#)
- [Upgrading CMD](#)
- [CMD Backup and Restore](#)

Additional Information

For emerging issues and other resources, see the following:

- The CMD [ReadMe](#).
- The CMD forum at www.storagecraft.com/support/forum.
- The StorageCraft technical support Web site at www.storagecraft.com/support.html.
- The [StorageCraft glossary](#).
- This User Guide is also available from the Help menu on the CMD console.

Documentation Conventions

 This symbol designates **Note** or **Warning** text that highlights important information about the configuration and/or use of ShadowControl CMD.

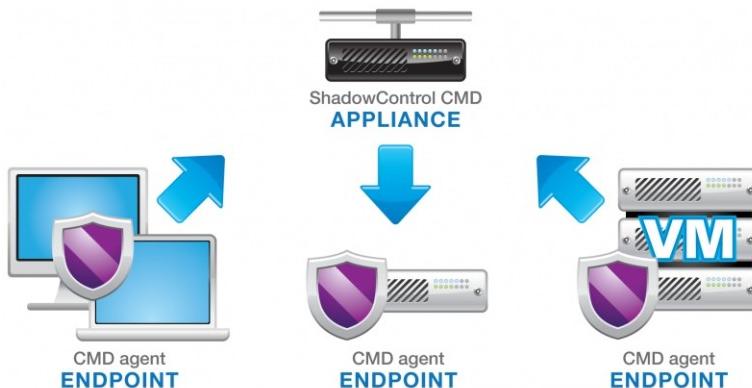
1 CMD Overview

Welcome to ShadowControl™ CMD—the superior monitoring tool for ShadowProtect-guarded networks! CMD delivers a central monitoring and reporting console for ShadowProtect and ImageManager operations, either for large sites or for MSPs with multiple clients. It also provides a critical secondary monitor on the ShadowProtect and ImageManager services in the event of either failing without notification.

Theory of Operations

CMD has two main components:

- [CMD Appliance](#)--a Linux-based server running as a VM or on dedicated hardware
- [CMD Agent](#)--a client installed at each EndPoint



CMD consists of EndPoints running the CMD agent and an appliance which monitors those Endpoints.

The CMD appliance receives status info from the CMD agent installed on each EndPoint.

Administration Schema

To supervise these components, CMD provides a granular schema for administrative roles. These roles differ primarily in the scope of the EndPoints they oversee:

- A **CMD SuperAdmin** manages the CMD appliance as well as add, edit, or remove all Organizations, Sites, EndPoints, user Accounts, and Rules applied to this specific appliance.
- An **administrator** can add, edit or remove sites as well as monitor all EndPoints for selected organizations on a specific appliance.
- A **Read-only** account on an appliance can view the status of EndPoints in one or more organizations or one or more sites on that appliance.

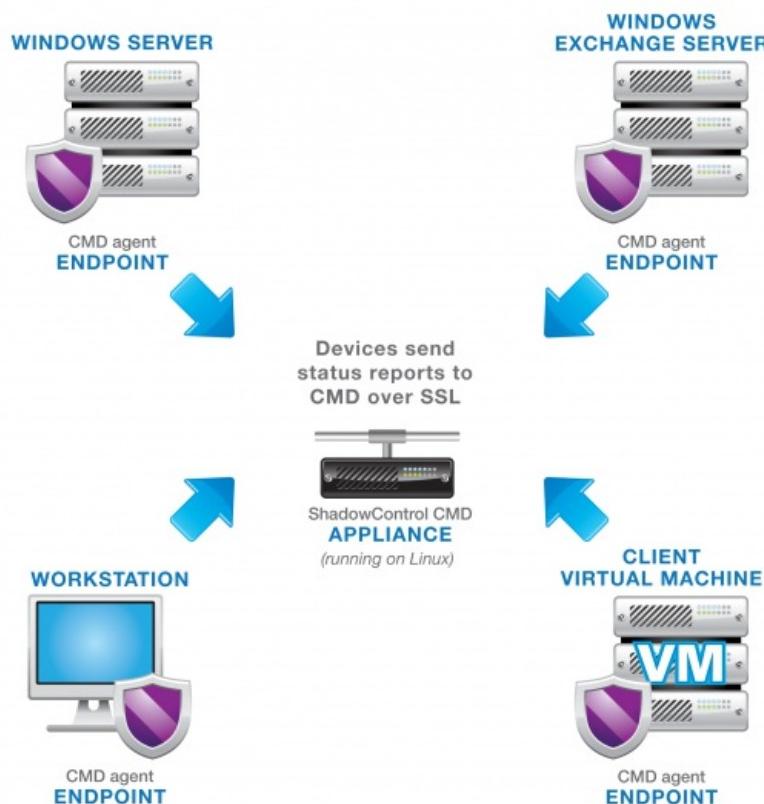
See [Administration](#) for further details on these roles.

1.1 CMD in Operation

To begin using CMD, an administrator would:

- Install the CMD appliance either on standalone hardware or as a virtual machine.
- Create one or more organizations to associate EndPoints with similar functions or locations.
- Create one or more sites within each organization to further associate EndPoints with similar requirements.
- Install the CMD agent on each ShadowProtect-guarded system.
- Assign each agent to an organization or to a site to monitor it using the CMD console.

The CMD appliance begins to receive a stream of status data over a encrypted link from each EndPoint every five minutes.



Each CMD EndPoint reports to the CMD appliance using SSL over Port 443 or 8443.

Status Rules

A major benefit of CMD is the ability to set alert thresholds--called *Status Rules*--on changes occurring in each EndPoint. Status rules can be set at the organization or the site level. Examples of status rules include the number of backup failures, online or offline status, and backup file size.

Using these status rules, the appliance can sort and display the EndPoints based on their condition:

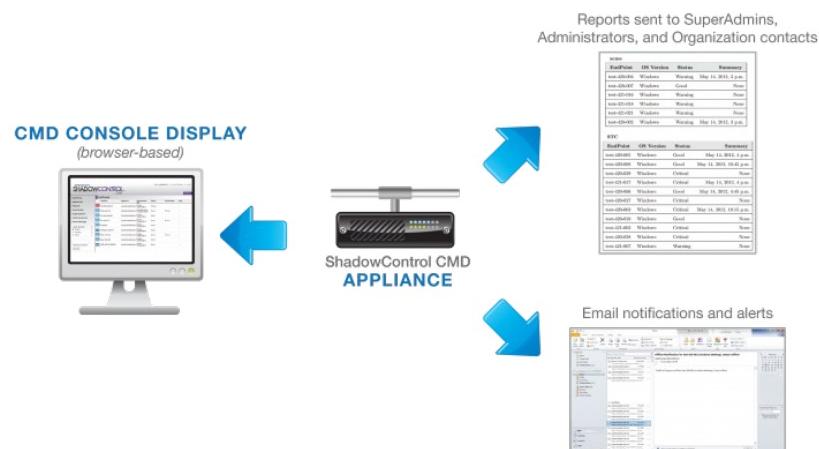
- **Good:** The EndPoint and backups are normal.
 - **Warning:** Activity on the EndPoint has exceeded one or more status rule thresholds set at the "Warning" level.
 - **Critical:** Activity on the EndPoint has exceeded one or more status rule thresholds set at the "Critical" level.
 - **Unresponsive/Offline:** The EndPoint is not reporting to the console.

Notifications

Another benefit of CMD is the ability to send email notifications when an EndPoint exceeds the status rule thresholds. CMD can send these notifications to either or both administrators and other contacts responsible for the affected EndPoint.

Reports

A final benefit is in scheduling reports. These reports can provide a range of content from a summary to a detailed backup report. CMD can send reports to administrators or other parties on a daily, weekly, or monthly schedule.



CMD displays EndPoint status information in the onscreen console as well as through email notifications and scheduled reports.

The CMD Appliance

The CMD appliance is the heart of CMD. As mentioned, this Linux-based server receives status reports from each CMD client-equipped EndPoint, providing details on its ShadowProtect and ImageManager installations, backup activity, and hardware configuration details. Administrators use the appliance's browser-based console to:

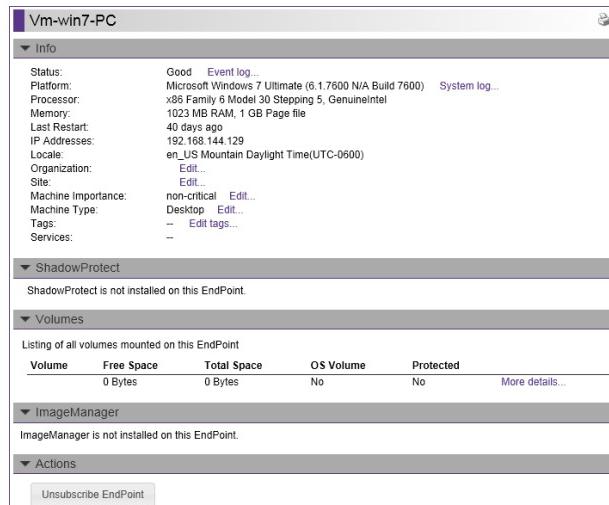
- Monitor EndPoints
 - Set status rules for EndPoints
 - Schedule reports

The appliance keeps a rolling 90-day log of EndPoint activity information for reporting purposes while each EndPoint maintains its own log. CMD provides an appliance backup function to preserve and restore the system history log In the event of an appliance failure.

The CMD EndPoint

Windows systems (both physical—servers, workstations, laptops—and virtual machines) can become EndPoints with the CMD agent installed. With the agent installed, each new EndPoint can subscribe to a CMD appliance and become a participating node in CMD.

Note: The CMD agent does not require ShadowProtect on the EndPoint. However, EndPoints that have ShadowProtect installed provide greater status details than systems with only the CMD agent.



The screenshot shows a software window titled "Vm-win7-PC". The "Info" section displays system details like Status (Good), Platform (Microsoft Windows 7 Ultimate), Processor (x86 Family 6 Model 30 Stepping 5, GenuineIntel), Memory (1023 MB RAM, 1 GB Page file), Last Restart (40 days ago), IP Addresses (192.168.144.129), Locale (en_US Mountain Daylight Time(UTC-0600)), Organization (Edit...), Site (Edit...), Machine Importance (non-critical), Machine Type (Desktop), Tags (-- Edit tags...), and Services (--). The "ShadowProtect" section indicates "ShadowProtect is not installed on this EndPoint". The "Volumes" section lists one volume: Volume (0 Bytes), Free Space (0 Bytes), Total Space (0 Bytes), OS Volume (No), Protected (No), and a "More details..." link. The "ImageManager" section states "ImageManager is not installed on this EndPoint". The "Actions" section contains a single button: "Unsubscribe EndPoint".

The CMD agent provides limited details when installed on a non-ShadowProtect-equipped EndPoint.

The CMD Portal

The CMD Portal is an optional component of most value only for sites with many appliances. The portal is a CMD appliance which acts as a supervisor for two or more subscribed appliances. Otherwise, it acts similar to the CMD console—displaying the status of EndPoints—with the added benefit that it does this for multiple CMD appliances rather than just one.

Administrators can use a portal to:

- Set system-wide status rules for all organizations or sites on the monitored appliances
- Create sets of organizations into Org Groups from various appliances
- Specify status rules for selected Org Groups
- Define system-wide or Org Group-specific reporting schedules

Note: Refer to [Portal Subscriptions](#) for details.

Dedicated Operation

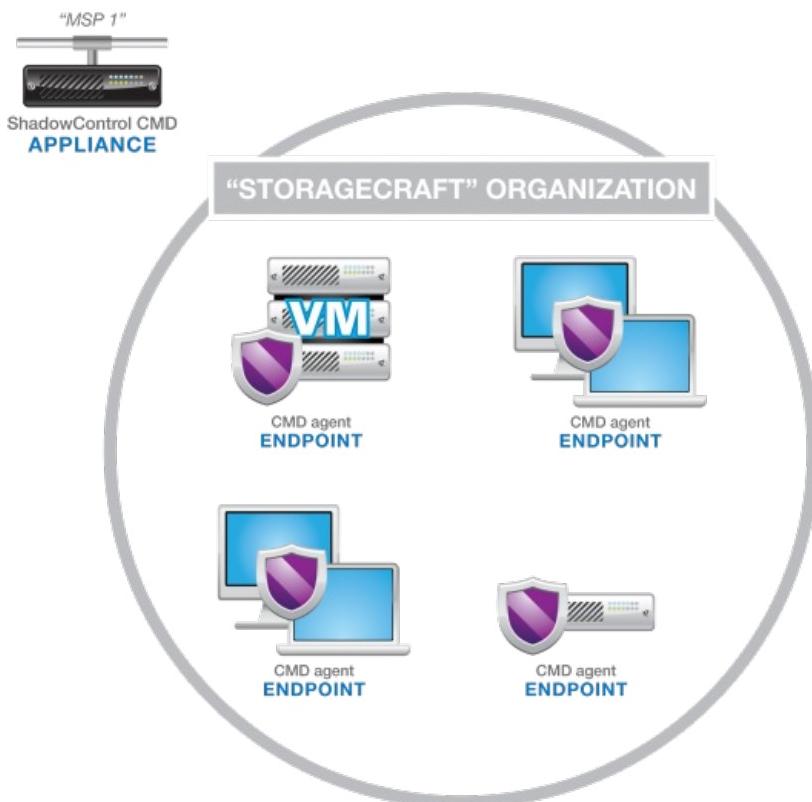
Although the Portal is a standard CMD appliance with the Portal feature activated, StorageCraft recommends that the Portal be a dedicated install of CMD rather than an "upgrade" of an existing appliance. However, if an existing CMD appliance is upgraded to run as a Portal, the original EndPoints will remain monitored by the Portal appliance. In that case, an additional navigation menu option will appear ("EndPoints") to display the list of monitored devices.

Org Groups

As CMD's span of control increases with multiple appliances, administrators can define sets of organizations into [Org Groups](#). These Org Groups can include one or more organizations from each of the subscribed appliances.

Organizations and Sites

CMD administrators can group EndPoints into organizations and sites for ease of management:



Note: Although "organization" and "site" imply a company name or physical location, these groupings can represent any common characteristic shared by a set of EndPoints. They can also represent a reporting group--where particular individuals need reports on the selected EndPoints.

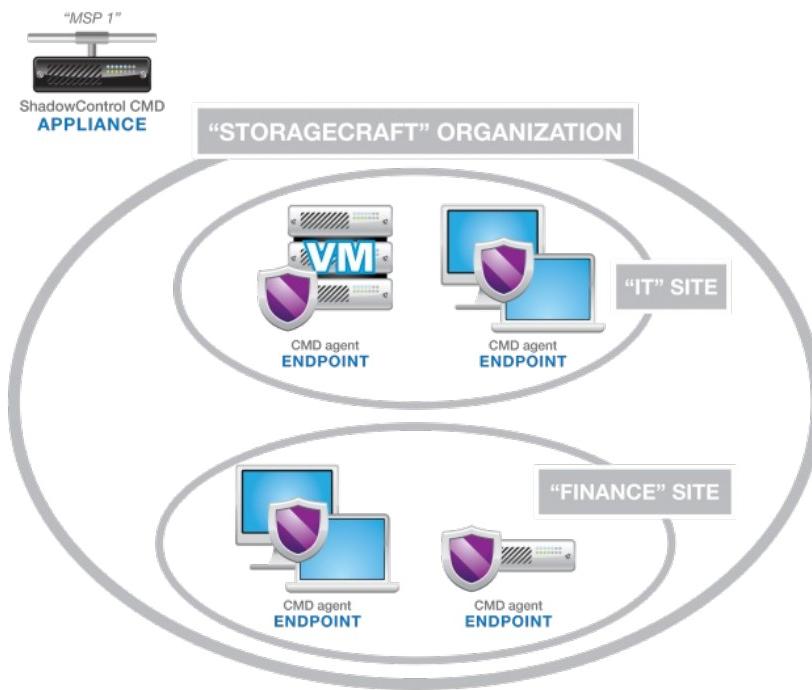
Each organization or site can also have its own set of Status Rules, allowing a high degree of granularity for alerts. For example, a "Servers" organization could have rules specific to their critical role, while a "Laptops" organization could have more lenient rules appropriate to that platform.

Default Organization and Site

The CMD appliance includes a Default Organization with a Default Site. CMD assigns all new EndPoints to this Default Organization and Site unless the EndPoints are assigned to a defined organization or site during the subscription process. We recommend assigning eachEndPoint to an appropriate organization or site rather than keep EndPoints in the Default Organization and Site.

Using Sites

A CMD organization can be further subdivided into one or more sites:

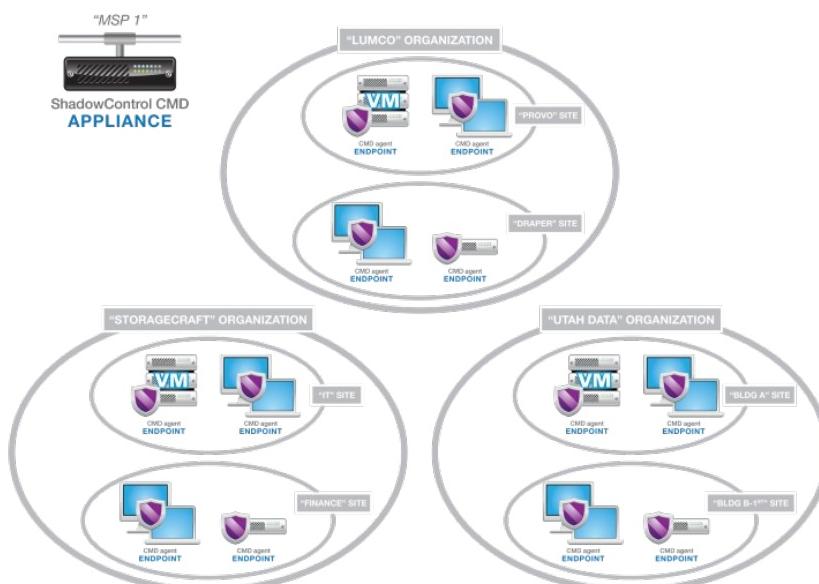


All EndPoints should belong to a defined organization. However, sites are an optional subdivision to an organization. Although optional, sites are useful in focusing attention on specific EndPoints within an organization. They also provide a convenient way to send different individuals (as contacts or administrators) notifications and reports based on their individual roles.

Again, while the name "Site" implies a physical location, a CMD site can represent any shared relationship or characteristic between a set of EndPoints. A relationship could include a company role, division, product, or location. A site could also represent characteristics such as operating system, application, or hardware type.

Multiple Organizations and Sites

Each appliance can support multiple organizations, each with its own set of sites (and each with its own set of status rules):

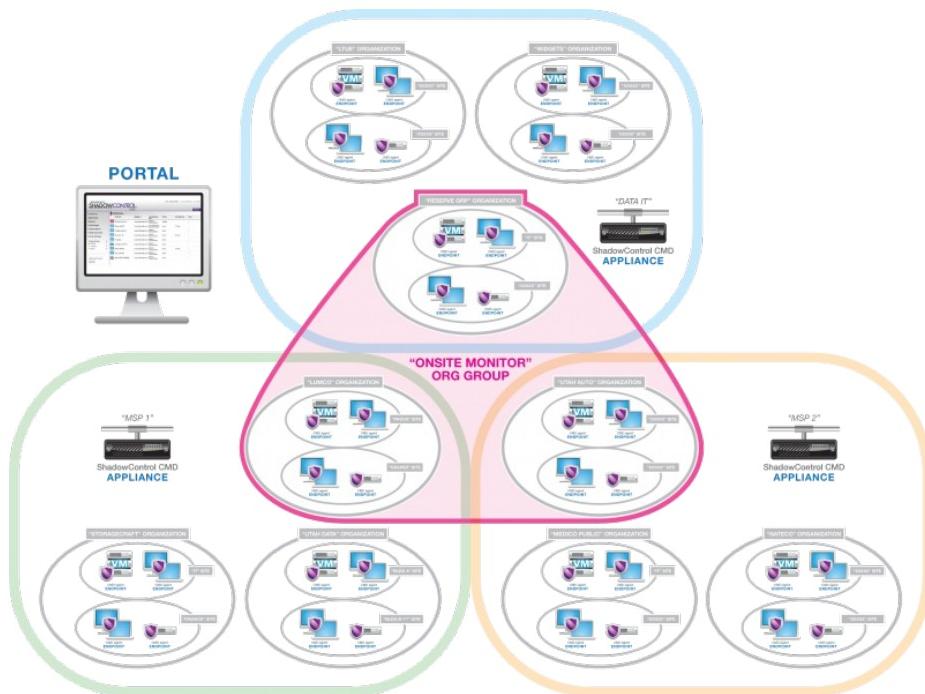


By defining multiple organizations and sites, administrators have a convenient way to send different individuals (as contacts or

administrators) notifications and reports based on their roles or area of responsibility. MSPs can define organizations and sites to closely match their client base and their EndPoints.

CMD Portal Org Groups

Administrators who implement a portal have an additional level of grouping called the *Org Group*. An Org Group is made up of selected sites and organizations from one or more monitored appliances:



Like an individual appliance's organization or site, a portal's Org Group can have separate status rules that flow down to each of its organizations and sites.

Note: Assigning status rules to an Org Group overrides any existing status rules applied at the appliance level to the sites or organizations that are part of the Org Group.

An Org Group can also have a separate set of contacts for notifications and reports.

Administration

As described earlier, CMD provides a granular schema for administrative roles:

- A **CMD SuperAdmin** manages the CMD appliance and can add, edit, or remove all organizations, sites, and EndPoints; and administer user accounts. The CMD superadmin can also set the Status Rules at the organization and site levels.
- An **administrator** can add, edit or remove sites as well as monitor all EndPoints for selected organizations on the appliance or portal.
- A **Read-only** account on an appliance can view the status of EndPoints in one or more selected organizations or one or more selected sites on that appliance. (A Read-only account created at the portal level is similar. A portal-level read-only account can view the status of EndPoints in one or more organizations or sites from one or more appliances.)

A typical CMD appliance would have one SuperAdmin and several administrators handling the organizations, sites, and EndPoints:



Administrators on a CMD appliance can monitor EndPoints in one or more organizations or sites.

The SuperAdmin can define as many administrators and read-only accounts as needed. (For example, additional read-only accounts can be for different personnel to receive notifications or reports.) The SuperAdmin can also assign additional users with SuperAdmin rights if needed to administer the appliance and appliance accounts.

Reports

CMD offers four possible sections in a report:

- **EndPoint Summary:** A general report on the monitored EndPoints
- **ShadowProtect EndPoint Details:** Provides backup job status information on each EndPoint
- **ImageManager EndPoint Details:** Lists the status of ImageManager-initiated jobs for each EndPoint.
- **Storage Statistics:** Lists the current disk space usage for backup files. It also has calculates a prediction of future space requirements. **Note:** CMD uses averages from the last 30 days to perform the calculation.

Reports can be sent to SuperAdmins, administrators, and to organization contacts on each appliance.

Report Scheduling

CMD can schedule reports:

- Daily (beginning of the day)
- Weekly (first day of the week)
- Monthly (first day of the month)

Note: Reports reflect a cumulative summary for the specified time period. CMD maintains a rolling 90-day log of endpoint activity for these report purposes and issues reports at 12:00AM.

The CMD Reports dialog displays a list of the last report sent of each type. Selecting a report in this list displays the archived content of that report.

Report Recipients

SuperAdmins and administrators designate the recipients and the type of report sent (Summary, Status, or Backup Status). The report's recipient dictates which set of EndPoints the report covers:

- **CMD SuperAdmins:** All organizations on a specific appliance.
- **CMD Administrators:** Reports on the administrators' designated sub-set of organizations on a specific appliance.
- **CMD Contacts:** Reports on an organization to the primary or secondary contact for that organization on a specific appliance.

CMD Scenarios

The concept of centrally monitoring ShadowProtect devices is extremely powerful, particularly for today's business environments where devices quickly multiply. CMD lets you keep tabs on these devices in ways that were previously not possible, as illustrated by the following usage scenarios.

Custom Rules

Problem: You need to keep track of different groups and types of machines across your organization. At the same time, you must have certain rules that apply to everyone and you don't want to manage them for each machine.

CMD Solution: ShadowControl CMD uses *Organizations* and *Sites* to create a hierarchy where you can set global rules, while maintaining custom monitoring where you need it.

- Set up your hardware and your organizations and sites.
- Set global status rules for your environment.
- Customize rules for the organizations and sites that need them.

For example, suppose you've organized your EndPoints by department and then by data priority, such as an "Accounting" organization with a subset of vital machines in a "Critical" site. You can set custom rules for the "Accounting" organization, then even more detailed rules for the subset of machines in the "Critical" site.

Device Priority

Problem: Your IT staff has only so much time. They can't always address every individual problem right away, but you know for sure that a problem with a server needs immediate attention while a problem with an employee laptop could be addressed later. You need a way to monitor what's happening by machine type.

CMD Solution: ShadowControl CMD gives you ways of seeing the status information you need. It's easy to distinguish between different machine types.

- Install the ShadowControl CMD agent on each server, desktop, and laptop. Subscribe each to a CMD appliance.
- In the ShadowControl CMD console, select each EndPoint and designate it as a Server, Desktop, or Laptop using the provided dropdown.
- Filter through your EndPoints on machine type. (Machine type serves as a predetermined tag for an EndPoint, allowing searches to find them when you need to.)

Senior Management Reports

Problem: It's budget time and executives have asked you to let them know how well your backup and disaster recovery plan performs. They need to know if it warrants continued investment. You need a way to generate a report that details your entire backup environment.

CMD Solution: ShadowControl CMD lets you create detailed reports for your entire business or any of your individual segments.

- Open the CMD console.
- Select the individual organizations and sites you want reports on. (Or, you can create reports for your entire backup environment.)
- Determine who should get the report. You can associate specific contacts with specific organizations and sites, so it's easy to make sure reports go to the right place. CMD sends reports on a schedule you define, but you can also generate them on demand.

2 Installing CMD

ShadowControl CMD installs as two components on separate systems:

- [The CMD Appliance](#): A Linux-based system installed on standalone hardware or as a Virtual Machine
- [The CMD Agent](#): A Windows-based client installed on each monitored device.

2.1 Installing the CMD Appliance

The CMD Appliance installs on standalone hardware or as a Virtual Machine. Both installations use the same ShadowControl_cmd ISO file.

System Requirements

Before installing the CMD appliance, make sure your system meets the following requirements:

- The CMD appliance is based on the 64-bit Ubuntu 12.04 operating system. If you choose to run the appliance on standalone hardware, please review [the Ubuntu 12.04 Supported Hardware Page](#) for detailed requirements for running Linux on various platforms.
 - The CMD appliance can also run as a virtual machine on:
 - Microsoft Hyper-V
 - VMWare Workstation
 - VMware ESX/ESXi
- Note:** Xen and Oracle VirtualBox are currently not supported.
- The appliance's CPU, disk space and RAM requirements are primarily determined by the number of EndPoints that subscribe to the Appliance. As a minimum for either a hardware- or VM-based appliance, we recommend:
 - 2GB RAM
 - 80GB disk space
 - Dual-core processor
 - Active Internet connection (to download server components during the install)
 - An available IP address (for remote console access) **Note:** This static IP address cannot be changed except by reinstalling the appliance.

- Either Port 443 or 8443 available (for EndPoint-to-appliance communication)
Note: Confirm that packet filtering also does not block communication from these ports.
- Port 5556 available (a required second port along with either 443 or 8443 for EndPoint-to-appliance communication)
- Port 25 or 587 available (if the optional email reporting is enabled)
- Supports EndPoints running ShadowProtect v4.2.7 or newer. (Older ShadowProtect versions do not correctly report their licensing information.)
- Supports monitoring StorageCraft ImageManager v6 or newer. (Upgrading ImageManager 5 to ImageManager 6 retains all premium job license features (HSR, iFTP, Cloud Services or ShadowStream).)

Using a Domain Hostname

You have the option to use a Domain Hostname rather than an IP address for subscribing EndPoints to the appliance. This allows you to change the appliance's IP address as needed without having to resubscribe EndPoints to that appliance. To use a hostname, however, you will first need to manually create a hostname entry on your DNS server for the appliance's IP address prior to installing CMD.

To install the CMD Appliance

1. Download the ShadowControl CMD ISO from the StorageCraft website.
Note: The Setup ISO is numbered differently from the release software. The Setup program will, however, install the latest version of the appliance.
2. Boot the physical or virtual machine using the ShadowControl_cmd ISO.
Note: If you are using a physical destination, first burn the CMD ISO to a CD.
3. Accept the default language of **English** for the Ubuntu install.
Warning: Selecting any other language instead of English prevents CMD from correctly installing. Remember, this language selection only affects Ubuntu. CMD uses the browser's default language for its interface.
4. Follow the remaining steps in the Installation Wizard to:
 - Specify a secure password for the SuperAdmin account.
 - Verify the necessary network information to install the CMD appliance: IP address, netmask, primary gateway, DNS servers, host name, and domain. Most CMD support issues come from incomplete or incorrect network settings. (The static IP address cannot be changed except by reinstalling the appliance.)

Note: The Install process can take 10 to 15 minutes or more as it downloads updates. The Install process might appear to hang, but this delay is normal.

After the CMD appliance finishes its start-up routine, it displays a login screen. At this point, the CMD appliance is running and all further configuration occurs through the browser-based CMD console. To access the console, open a browser to <https://IPaddress> where *IPaddress* is the address you gave the CMD appliance during the installation.

Note: If you need to reboot or shutdown the appliance, you can do so from the CMD console.

2.2 Installing the CMD Agent

You must install the CMD agent software on each device you want to monitor. The EndPoint agent is found in the CMD directory. (The default is C:\Program Files (x86)\StorageCraft\cmd.)

System Requirements

- CMD client's hardware and software requirements are the same as for [ShadowProtect](#).
- CMD supports ShadowProtect versions 4.2.7 and newer. (Remote licensing requires ShadowProtect 4.2.5 or newer.)
- CMD monitors StorageCraft ImageManager 6 and newer.
- The agent communicates with the CMD appliance using two required ports: either Port 443 or 8443 (selectable during installation) and Port 5556.

Note: While you can monitor devices that do not have ShadowProtect installed, CMD only provides minimal detail on those systems.

Warning: CMD v1.1.1 and newer does not support Windows 2000 EndPoints. Furthermore, legacy CMD client software for Windows 2000 will not interoperate with CMD v1.1.1 or newer appliances. Use the ShadowProtect console's management tools to monitor Win2K EndPoints as an alternative.

You can install the CMD agent:

- [Directly on the EndPoint](#)
- [Via Silent Install](#)

Note: All EndPoints must be manually upgraded to v2.0. CMD can perform automated updates for 2.0 and newer EndPoints.

Subscribing to the CMD appliance occurs automatically when installing directly on the EndPoint. When using the Silent Install, you can [manually subscribe the EndPoint](#) to the CMD appliance from the command line.

Working with Non-VSS Systems

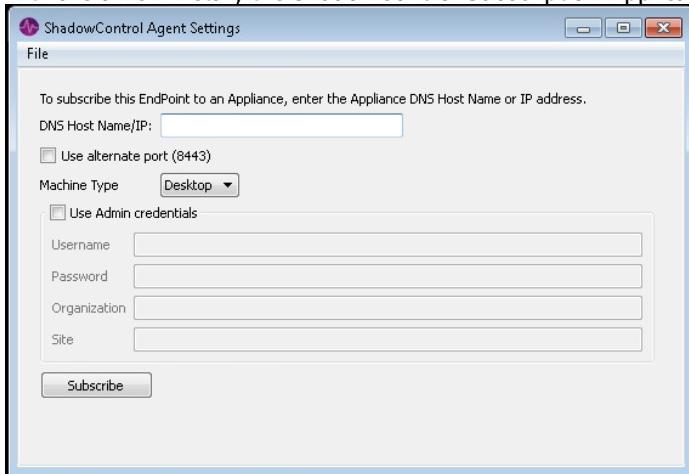
Some EndPoints may not support VSS backups. On these non-VSS systems, an optional CMD ShadowProtect Rule produces an alert for each non-VSS backup. When active, this rule results in a continuous flow of notifications for these non-VSS EndPoints. To avoid this when using this policy rule:

1. Create an organization or site for these devices. Name this group "*Non-VSS Systems*" or similar.
2. Group all non-VSS systems into this site or organization.
3. Select the non-VSS site or organization and open its *Status Rules* page.
4. Confirm that the **Last VSS Backup** rule is unchecked. This prevents the issuing of notifications for these EndPoints. EndPoints that do use VSS can keep the Non-VSS rule and generate alerts if VSS fails.

EndPoint Install

To install the agent directly on the EndPoint:

1. Download and unpack *ShadowControl_CMD_Setup_x.x.zip*, where *x.x* is the product version number.
2. Click on the *ShadowControl_Installer.msi* file.
3. On the Welcome page, click **Next**.
4. On the License Agreement page, select **I accept the terms of the license agreement**, then click **Next**.
Note: You must accept the license agreement to install CMD.
5. Click **Next** to accept the default destination folder for the agent.
6. On the Ready to Install page, click **Install**.
7. When the install completes, the wizard displays the option to *Launch ShadowControl Subscription Application*. This option allows the user to specify the CMD appliance to subscribe to. Accept the default if this is a new agent install. If it is an upgrade, uncheck the box.
8. Click **Finish**.
9. If this is a new install, the ShadowControl Subscription Application appears:



On the *ShadowControl Agent Settings* page, specify the required information:

DNS Host Name/IP	The hostname or IP address of the CMD appliance where you want to subscribe this endpoint.
Use alternate port (8443)	Check Use alternate port (8443) to have the EndPoint communicate with the CMD appliance on port 8443 if the default SSL port (443) is already in use.
Machine Type	Enter the endpoint's type, or class. Options include Desktop , Laptop , Server , and Virtual . CMD uses this information to classify systems within its interface.

Use Appliance Admin credentials	enroll the endpoint. If you do not provide valid credentials or enrollment information, the new EndPoint appears in the list with a request to Approve or Deny its subscription. A CMD administrator or superadmin must approve the new EndPoint to complete the subscription. CMD does not monitor this EndPoint until approved.
--	--

10. Click **Subscribe**.

When the subscription completes, the EndPoint appears in the list of subscribed devices on the selected appliance.

Note: If the Machine Type changes (Server, Desktop, Laptop, or Virtual Machine), use the [Info section](#) of the EndPoint Details page to change it.

Working with Non-VSS Systems

Some EndPoints may not support VSS backups. On these non-VSS systems, an optional CMD ShadowProtect Rule produces an alert for each non-VSS backup. When active, this rule results in a continuous flow of notifications for these non-VSS EndPoints. To avoid this when using this policy rule:

1. Create an organization or site for these devices. Name this group "*Non-VSS Systems*" or similar.
2. Group all non-VSS systems into this site or organization.
3. Select the non-VSS site or organization and open its *Status Rules* page.
4. Confirm that the **Last VSS Backup** rule is unchecked. This prevents the issuing of notifications for these EndPoints. EndPoints that do use VSS can keep the Non-VSS rule and generate alerts if VSS fails.

This prevents the issuing of continuous notifications for these EndPoints. EndPoints that do use VSS, however, keep the Non-VSS rule and generate alerts if VSS fails.

Silent Install

You can also perform a silent install of the CMD agent. This is useful to push the agent out to EndPoints via a policy.

The CMD agent silent Install command syntax is:

```
msiexec.exe /quiet /i ShadowControl_Installer.msi
```

Run this command from the folder with the Installer msi or include the path (ie: C:\Program Files (x86)\StorageCraft\CMS\ShadowControl_Installer.msi).

Subscribing the EndPoint

When performing a Silent Install, you can [manually subscribe the EndPoint](#) to the CMD appliance from the command line to monitor the EndPoint.

Manual Subscription

The majority of EndPoint subscriptions occur using the install Wizard. In some cases, however, the EndPoint may require a manual subscription to a ShadowControl appliance. (For example, as part of a Silent Install.)

To perform a manual subscription of an EndPoint to an appliance:

1. Run a command prompt as Administrator on the unsubscribed EndPoint.
2. Navigate to where CMD is installed. (The default is Program Files (x86)\StorageCraft\CMS.)
3. Enter the command:

```
stccmd.exe subscribe <IP address/Server Name>
```

where *IP address* is the address to the appliance and *Server Name* is the DNS name. Use either the address or the server name if the appliance is on an external address.

The EndPoint Agent subscribes to the specified ShadowControl appliance.

Note: An EndPoint agent can subscribe to only one appliance at a time.

Command Line Options

The agent supports various options for appliance connections using the *stccmd* command:

Option	Description
<i>-o</i>	Specifies the EndPoint's Organization and optionally the Site.
<i>-m</i>	Specifies the EndPoint's System Type (server, desktop, virtual, laptop). (Note that this is case sensitive.)
<i>-U</i>	Specifies the appliance's username. Use the <i>-P</i> option to specify a password if needed. Note: This is the only way to create an EndPoint's username and password without rerunning the installation.
<i>-P</i>	Specifies the appliance's user password. Must be used in conjunction with the <i>-U</i> option.
<i>-t</i>	Identifies any desired Tags for this EndPoint.
<i>-a</i>	Forces the EndPoint and appliance to communicate using the alternative port 8443.

These options can be combined as needed:

Task	Command Example	Description
Subscribe the EndPoint to an appliance on the same local network	<i>stccmd.exe subscribe 192.0.0.2</i>	Use the local IP address for onsite EndPoints. Use the external IP address or DNS name for an offsite CMD appliance.
Subscribe the EndPoint using the alternate port 8443	<i>stccmd.exe subscribe -a TestCMD</i>	Subscribes the EndPoint to the "TestCMD" appliance using Port 8443. Specify the appropriate server name or its IP address when used.
Resubscribe the EndPoint to the appliance where the EndPoint previously subscribed.	<i>stccmd.exe resubscribe TestCMD</i>	Resubscribes the EndPoint to the "TestCMD" appliance. Specify the appropriate server name or its IP address when used.
Unsubscribe the EndPoint from an appliance	<i>stccmd.exe unsubscribe</i>	Since an EndPoint can only subscribe to one appliance, the command does not require the appliance's IP address.
Force the EndPoint to unsubscribe from an appliance	<i>stccmd.exe unsubscribe -f</i>	May be required if the appliance is not accessible.
Subscribe the EndPoint using a tag	<i>stccmd.exe subscribe -t WinXP</i>	Subscribes the EndPoint and attaches the tag "WinXP" for use in sorting the EndPoint List.

Manually specify an organization and site for the EndPoint subscription

```
stccmd.exe subscribe -o my_org:my_site -U username -P password
```

This example subscribes the EndPoint to the "my_org" organization, then assigns it to the "my_site" site. (If subscribing to only an org, leave off ":site" in the command.) Assigning an EndPoint to an organization or site requires the desired CMD appliance's "username" and "password" in the command.

Manually specify an EndPoint type

```
stccmd.exe subscribe -m server
```

Identifies the system as a "server" type in the EndPoint list.

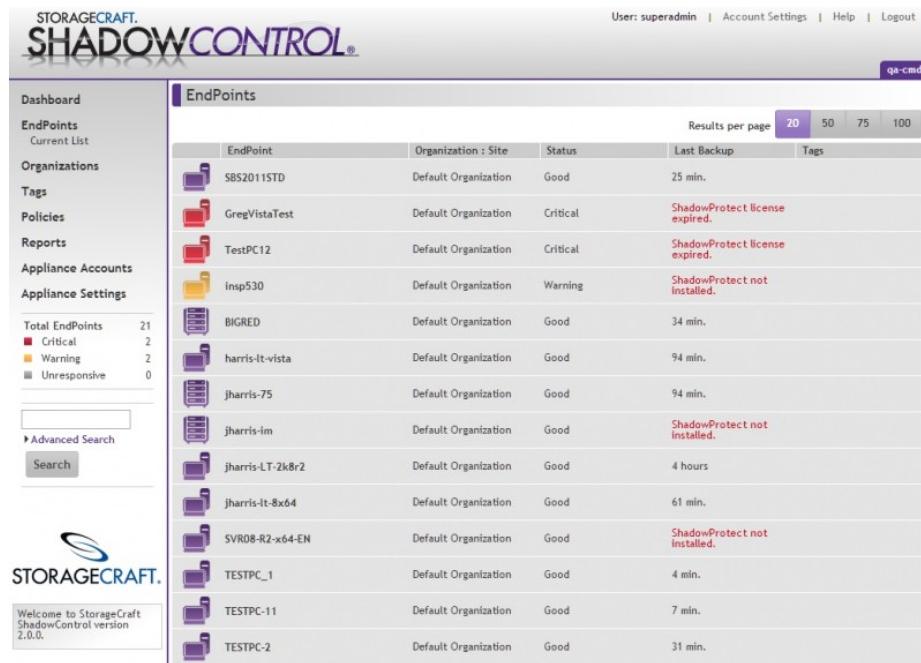
Manually specify an appliance, username, password, organization and site, and EndPoint type during the subscription.

```
stccmd.exe subscribe 192.0.0.2 -U CMDAdmin -P XL5stor -o my_org:my_site -m server
```

Subscribes the EndPoint to the appliance at IP address 192.0.0.2 using credentials CMDAdmin and password XL5stor. The EndPoint is inserted in the "my_org" organization under the site "my_site" as a "server" type.

3 Understanding the CMD Console

The CMD console displays current EndPoint status information and provides access to the configuration and operating controls for CMD:



The screenshot shows the StorageCraft ShadowControl CMD interface. The left sidebar contains navigation links: Dashboard, EndPoints Current List, Organizations, Tags, Policies, Reports, Appliance Accounts, and Appliance Settings. A summary table shows Total EndPoints (21), Critical (2), Warning (2), and Unresponsive (0). Below this is an Advanced Search button and a Search button. The main panel displays a table titled "EndPoints" with columns: EndPoint, Organization : Site, Status, Last Backup, and Tags. The table lists 15 endpoints, each with a small icon and status details. At the top right of the main panel, there are links for User: superadmin | Account Settings | Help | Logout, and a dropdown menu labeled "qa-cmd".

EndPoints									
					Results per page	20	50	75	100
	SBS2011STD	Default Organization	Good	25 min.					
	GregVistaTest	Default Organization	Critical	ShadowProtect license expired.					
	TestPC12	Default Organization	Critical	ShadowProtect license expired.					
	insp530	Default Organization	Warning	ShadowProtect not installed.					
	BIGRED	Default Organization	Good	34 min.					
	harris-lt-vista	Default Organization	Good	94 min.					
	jharris-75	Default Organization	Good	94 min.					
	Jharris-im	Default Organization	Good	ShadowProtect not installed.					
	jharris-LT-2k8r2	Default Organization	Good	4 hours					
	Jharris-it-8x64	Default Organization	Good	61 min.					
	SVR08-R2-x64-EN	Default Organization	Good	ShadowProtect not installed.					
	TESTPC_1	Default Organization	Good	4 min.					
	TESTPC-11	Default Organization	Good	7 min.					
	TESTPC-2	Default Organization	Good	31 min.					

The console is divided into three panels:

Navigation Panel: Located at the left side of the console, the Navigation panel provides options for tasks and configuration needed to monitor subscribed EndPoints. (For more information, see [Navigation Panel](#).)

Main Panel: Located at the center of the console, the Main panel displays the CMD Dashboard (by default) or lists of EndPoints or configuration details. (For more information, see [Main Panel](#).)

Session Panel: Located at the top right of the console, the Session panel displays the current username and appliance as well as session options. (For details, see [Session Panel](#).)

3.1 Navigation Panel

The left-side Navigation panel provides access to CMD status and tools:



The items include:

Option	Function
Dashboard	Displays the current status of each monitored EndPoint for ShadowProtect, ImageManager, and ShadowControl agent notifications. (This is the Main Panel's default view.) (See Dashboard for more information.)
EndPoints	Displays a list of subscribed devices to the appliance in the Main Panel. This option updates to display the name of each subsequent page in the hierarchy as the user drills down through the list to view additional details, including the name of a selected EndPoint. (See EndPoint List for more information.)
Organizations	Displays a list of organizations and sites currently defined on the appliance. Use this option to add, edit, or remove organizations and sites on the appliance; or to view and modify the Status Rules for a selected organization or site (See Using Status Rules for more information.) Note: CMD will not delete the Default Organization. However, administrators can modify the Default Organization's Status Rules.
Tags	Opens the Tags dialog. This dialog displays the list of existing user-defined tags with the option to create, edit, or delete tags. Tags simplify EndPoint searches as a filter to display only those sharing a common characteristic or role. (See Tags for details.)

Policies	system. These status rules govern when CMD displays and reports alerts concerning EndPoint issues. (See Policies for more information.)
Reports	Displays report settings and an archived report list. (See Reporting for more information.)
Appliance Accounts	Displays a list of users for this appliance to add, edit, or remove users. (See Appliance Accounts for more information.)
Appliance Settings	Displays the appliance's settings. (See Appliance Settings for more information.)
EndPoint Summary	(Does not display when viewing the Dashboard.) Shows the number of EndPoints with a breakdown of their condition. (See EndPoint Summary for more information.)
Search	A search field which displays a list of EndPoints that match specified search terms or criteria. (See Search for more information.) Note: Search only appears when <i>EndPoints</i> is selected in the Navigation panel.
Newsfeed	Displays a scrolling list of messages about StorageCraft and ShadowControl CMD. (This feature is available in English only.)

Organizations

The Organizations option displays a list of the currently-defined organizations and their sites on this appliance. Organizations are collections of EndPoints. Sites are a subcollection of EndPoints from an Organization that share common settings or a common location.

Organizations

Organizations are collections of EndPoints. Sites are a subcollection of EndPoints from an Organization that share common settings or a common location. To add a site to an organization, select 'Add Site' from the Actions column.

<input type="checkbox"/> Organization / Site	EndPoint Count	Actions
<input type="checkbox"/> BDR	1	   
<input type="checkbox"/> Draper	0	 
<input type="checkbox"/> Ireland	0	 
<input type="checkbox"/> Desktops	3	   
<input type="checkbox"/> Servers	2	   
<input type="checkbox"/> Default Organization	0	 

[Add Organization](#)

The list displays:

Column	Description
Organization/Site	Shows the organization's name and any sites that are part of it.
EndPoint Count	For organizations, lists the total number of EndPoints subscribed to an organization. For sites, lists the number of EndPoints assigned to the site.
Actions	Displays icons for functions available to manage a site or organization.
Add Organization	Click Add Organization to create a new one.
Edit Rules	Checkmark an organization or site, then click Edit Rules to manage the status rules for that set of EndPoints.

Note: You cannot delete or assign EndPoints to the Default Organization.

Actions

The Action options include:

Icon	Description	Function
	Add site icon	Opens a dialog to configure a new site for the organization.

	Assign EndPoints icon	Displays a filtered list of available EndPoints. Checkmark one or more to add them to the site or organization.
	Blue pencil icon	Opens the selected organization's configuration page. Use this page to edit the name, contacts, or status rules. (See Using Status Rules for more details.)
	Red delete icon	Deletes the selected organization. EndPoints that were part of the deleted organization revert back to the Default Organization. Note: You cannot delete the Default Organization.

Assigning EndPoints

When you click the Assign Endpoints icon, CMD displays a filtered list. By default, it shows the list of EndPoints from the Default Organization:

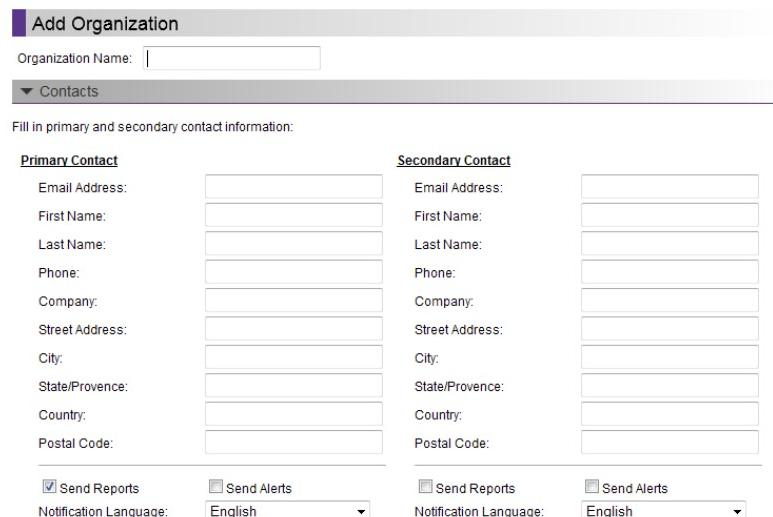


You can modify the list of EndPoints using the filtering options:

Filter	Description
Organization	Displays all EndPoints matching the selected organization from the dropdown box. Initially, this is the Default Organization. EndPoints marked with a checkmark are members of the selected organization in the previous dialog.
Tag	Displays all EndPoints labeled with the selected tag from the dropdown box.
All EndPoints	Displays all EndPoints subscribed to this appliance. Those EndPoints already assigned to the selected site or organizations have a checkmark.

Add Organization

Click **Add Organization** to add a new organization:



To add a new organization:

- Type in a name for the new organization. Select a name that reflects the shared characteristic of the EndPoints in this group. This could be a location ("Second Floor"), or it could be a department ("Finance") or a platform ("Laptop" or "Windows 2K").
- Note:** Both organization and site names support non-English characters. They do not, however, support control characters such as "&", "?" and similar.

2. If the organization has separate contacts (in addition to the administrator), type in their information. By typing in valid email addresses, these contacts can also receive reports on the site's EndPoints.
3. Select to send the contact either or both reports and alerts.
4. Select the contact's preferred language so CMD sends the report in the appropriate language.
5. Decide to:
 - a. Use the Default Organization's status rules (the default selections under Status Rules) or to
 - b. Create a set of custom rules for this organization.

See the section on [Using Status Rules](#) for more information on configuring rules.

6. Click **Save** to save the new organization.

New EndPoints can now enroll into this organization or the administrator can edit an existingEndPoint's settings to make it a member of this organization.

Edit Organization Status Rules

All organizations inherit their status rules from the Default Organization on the appliance. To edit these rules:

1. Select an organization in the list using the checkbox next to its name.
2. If you want to edit the rules for all of the organizations, check the box next to *Organizations* at the top.
3. Click **Edit Rules** to view the selected organization's status rules and modify them.
4. Click **Save** to keep the changes.

See [Using Status Rule Policies](#) for more information.

Sites

Organizations are collections of EndPoints. Sites are a subcollection of EndPoints from an Organization that share common settings or a common location.

To add a site to an organization:

1. Click **Organizations** in the navigation panel.
2. Select an organization to add a site to.
3. Click  in the organization's Actions column. CMD displays the *Add Site* dialog:

Add Site

Site Name:	<input type="text"/>
Organization:	Americas
Contacts	
Fill in primary and secondary contact information:	
Primary Contact	Secondary Contact
Email Address:	<input type="text"/>
First Name:	<input type="text"/>
Last Name:	<input type="text"/>
Phone:	<input type="text"/>
Company:	<input type="text"/>
Street Address:	<input type="text"/>
City:	<input type="text"/>
State/Provence:	<input type="text"/>
Country:	<input type="text"/>
Postal Code:	<input type="text"/>
<input checked="" type="checkbox"/> Send Reports	<input type="checkbox"/> Send Alerts
Notification Language:	English
<input type="text"/>	Notification Language: English

3. Type in a name for the new site. Select a name that reflects the shared characteristic of the EndPoints in this group. This could be a location ("Second Floor", "London", etc), or it could be a department ("Finance", "Sales", etc) or a platform ("Windows XP", "Windows 7" etc).

Note: Site names support multi-lingual characters. However, these names do not support reserved control characters such as "&", "?" or similar.

4. Type in contact information for either a primary or secondary contact if the site has separate contacts (as opposed to the administrator).
5. Select to send either of these contacts CMD reports or email alerts. Note: The contact must have a valid email address listed to receive CMD reports.
6. Specify the contact's preferred language for reports and alerts.
7. Decide to either use the organization's Status Rules or to define custom rules for this site. (See [Using Status Rules](#) for details.)
8. Click **Save** to save the new site.

New EndPoints can now enroll into this site or the administrator can edit an existing EndPoint's settings to make it a member of this site.

Tags

This dialog displays the list of existing user-defined tags with the option to create, edit, or delete tags.

The screenshot shows a software interface titled "Tags". At the top right is a "Create Tag" button. Below it is a horizontal list of four tags: "FT Bldg", "ImageReady", "UEFI MoBo", and "Windows 8", each followed by a small edit icon and a trash bin icon.

Tags simplify EndPoint searches as a filter to display only those sharing a common characteristic or role.

To create a tag:

1. Enter a name.
2. Click **Create Tag**.

CMD also supports adding tags directly from the [EndPoint Details Info](#) section.

Note: Tags support multi-lingual characters.

Renaming Tags

Click to change the tag's name. CMD updates the name and preserves the link to all EndPoints using this tag.

Deleting Tags

Click to delete the tag. CMD also removes the deleted tag from all EndPoints previously using it.

Reports

CMD can generate cumulative reports at these intervals:

- Daily
- Weekly
- Monthly

It can send these reports to:

- SuperAdmin
- Administrators
- Organization Contacts

The Reports option also displays a list of the most recently generated reports for the last 30 days. It also displays additional information including a detailed list of ShadowProtect licensing.

See [Reporting](#) for more information.

Appliance Accounts

Appliance Accounts displays a list of the defined users for the appliance:

Accounts				
Username	Email	Role	Organizations	Actions
dad	dad@example.com	Superadmin		
lara	lara@example.com	Admin		
superadmin	john.harris@storagecraft.com	Superadmin		

[Add User](#)

Actions

You have two actions available when working with a selected user account:

Icon	Description	Function
	Pencil icon	Opens the selected account's configuration page. Use this page to edit the user's name, email address, language or role.
	Trash can icon	Deletes the selected user account. Note that CMD will not delete the currently logged-in user or the superadmin account.

Add User

The Add User button opens a page where you can add a new user to the appliance.

[Add User](#)

Configure user account settings for logging into this appliance.

Username:	<input type="text"/>
Password:	<input type="password"/>
Confirm Password:	<input type="password"/>
Email:	<input type="text"/>
Preferred Language:	<input type="button" value="English"/>
Choose a role to set the new user's access: Superadmin - grants full access. Admin - grants access to manage only assigned Organizations. Read Only - grants read-only access to assigned Organizations.	
Role:	<input type="button" value="Superadmin"/>
<input type="button" value="Save"/>	

To add a user:

1. Type in a name, password, and valid email address for the user. (The email address is optional, but without it the user does not receive notifications.)
2. Select a preferred language for reports and notifications sent to this user.
3. Select the user role.
4. Selecting either the *Admin* or *Read Only* user role displays a list of available organizations to assign to this user:

Role:

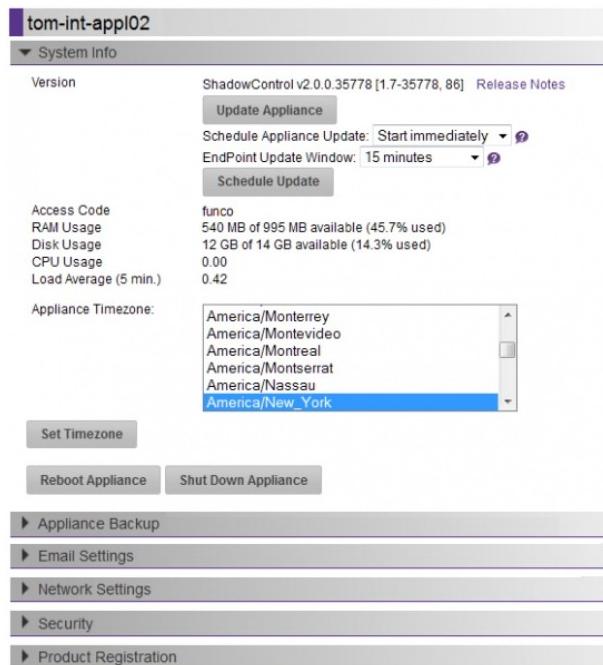
Organizations: Acme
 QA Division
 STC Corp

4. To assign an organization to the new user, mark the checkbox next to one or more of the listed organizations.
5. Click **Grant Access**. (Use **Remove Access** to unassign an organization for this user.)

6. Click **Save** to create the new user account.

Appliance Settings

The Appliance Settings option in the Navigation panel displays the system's current settings:



The screenshot shows the 'System Info' section of the Appliance Settings interface. It includes:

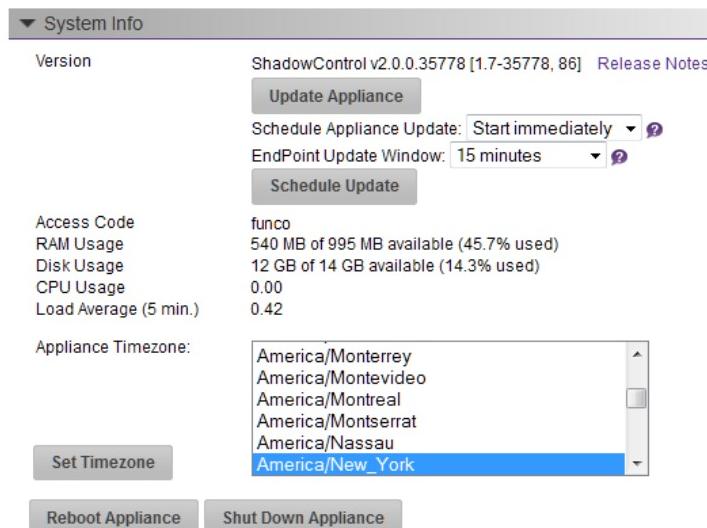
- Version:** ShadowControl v2.0.0.35778 [1.7-35778, 86] [Release Notes](#)
- Update Options:**
 - Update Appliance** button
 - Schedule Appliance Update: **Start immediately** dropdown
 - EndPoint Update Window: **15 minutes** dropdown
 - Schedule Update** button
- System Status:**
 - Access Code: func0
 - RAM Usage: 540 MB of 995 MB available (45.7% used)
 - Disk Usage: 12 GB of 14 GB available (14.3% used)
 - CPU Usage: 0.00
 - Load Average (5 min.): 0.42
- Appliance Timezone:** A dropdown menu listing timezones, with **America/New_York** selected.
- Action Buttons:** **Set Timezone**, **Reboot Appliance**, **Shut Down Appliance**.
- Navigation Panel:** Includes links for **Appliance Backup**, **Email Settings**, **Network Settings**, **Security**, and **Product Registration**.

The sections include:

- [System Info](#)
- [Appliance Backup](#)
- [Email Settings](#)
- [Network Settings](#)
- [Security](#)
- [Product Registration](#)

System Info

System Info provides details on the CMD appliance and options to control the server:



The screenshot shows the 'System Info' section of the Appliance Settings interface. It includes:

- Version:** ShadowControl v2.0.0.35778 [1.7-35778, 86] [Release Notes](#)
- Update Options:**
 - Update Appliance** button
 - Schedule Appliance Update: **Start immediately** dropdown
 - EndPoint Update Window: **15 minutes** dropdown
 - Schedule Update** button
- System Status:**
 - Access Code: func0
 - RAM Usage: 540 MB of 995 MB available (45.7% used)
 - Disk Usage: 12 GB of 14 GB available (14.3% used)
 - CPU Usage: 0.00
 - Load Average (5 min.): 0.42
- Appliance Timezone:** A dropdown menu listing timezones, with **America/New_York** selected.
- Action Buttons:** **Set Timezone**, **Reboot Appliance**, **Shut Down Appliance**.

These include:

Item	Description
Version	Reports the software version for the CMD appliance (not the Linux version it runs on).
Release Notes	Click this button to display the CMD ReadMe file. Since the CMD update process is automatic, viewing this file allows administrators to note new software requirements or changes to CMD prior to installing the update.
Update Appliance	Click this button to perform an automatic update to the appliance. (View the CMD ReadMe to see what enhancements come with the update.) Note: This button only appears when CMD detects an update to the appliance software.
Schedule Appliance Update	This button only appears after clicking Update Appliance . Use this option's <i>Schedule Appliance Update</i> dropdown box to perform the appliance update immediately or at a later time.
EndPoint Update Window	This dropdown box only appears after clicking Update Appliance . Use it to set the time when the automated updating of EndPoint agents should end; or to mandate a manual update of each agent. CMD then updates each agent at random intervals in the selected time. This prevents saturating network bandwidth. Note: Automated updating is supported only with CMD EndPoint agents v2.0 or newer.
Access Code	Displays the user-defined code (set during the install) that may be used by StorageCraft Support in troubleshooting appliance issues. Treat this as similar to a password.
RAM Usage	Displays the amount of RAM the CMD appliance is using. Note: The percentage references the Linux OS RAM usage, not the CMD appliance.
Disk Usage	Displays the amount of disk space used by the CMD appliance.
CPU Usage	Displays the appliance's current CPU utilization.
Load Average	Shows the average work load on the CPU over the last five minutes. As a baseline, an average of 1.00 is 100% utilization of a single core, a 2.00 is 100% of two cores, etc. Monitor this to keep the average under the maximum for the number of cores installed (if a dedicated system) or the number assigned to CMD (if a virtual machine).
Appliance Timezone	Use the selector box to find and highlight the appliance's timezone. Click Set Timezone to accept it.
Reboot Appliance	Click this button to reboot the appliance if a reboot is necessary. (The CMD appliance does not have command line access so it can't be used for reboots.)
Shut Down Appliance	Click this button to gracefully shutdown the appliance.

Email Settings

Email Settings specifies the SMTP server used to send notifications regarding EndPoint issues as well as the branding used in notifications:

Configure SMTP server settings used to send reports and alert notifications.

Use this appliance's built-in SMTP server.

From Address: storagecraftalert@gmail.com

Use another SMTP server.

Host Name or IP Address:

Port:

Username:

Password:

From Address:

Security: Use TLS

Don't use an SMTP server. (Warning: if this option is selected, no email will be sent from this appliance)

Customize reports and alert notifications with corporate branding.

Name: ShadowControl CMD

Logo: Image must be in JPEG or PNG format and will be scaled down to a maximum size of 250x100 pixels.

Upload custom logo No file chosen

Use default logo

Current Logo: 

To configure the email settings:

1. Choose whether to use the default CMD SMTP server, an existing SMTP server, or no SMTP server.
Note: There may be circumstances when you do not want to configure an email server (such as part of a test). However, we recommend that each appliance have an SMTP server configured for sending email notifications.
2. Keep the selected *Built-in SMTP* option to use CMD's SMTP server.
3. Enter an address in the *From Address* field. (This does not have to be a valid address.)
4. Select *Use another SMTP server* to send notifications with an existing server.
5. Specify this other server's settings including credentials.
Note: ShadowControl uses Port 25 by default. If necessary, substitute Port 587 if ShadowControl fails to send email reports.
6. Enter an address in the *From Address* field.
7. Choose whether to use TLS.
8. Select *Don't use an SMTP server* if you choose to run a test on CMD.
9. Click **Save**.
10. Click **Send Test Email** to confirm the connection.

Note: Sometimes email sent from the CMD server may bounce or be routed to a Spam folder on the destination system. Click **Send Test Email** to determine if this is the case. If so, configure CMD to use an existing SMTP server.

To have a different branding appear on CMD reports and notifications:

1. Specify a name for this branding (for example, XYZ MSP Services).
2. Check *Upload custom logo*, then click **Choose File** to upload an image file (or keep the default logo). CMD will display a sample of the chosen logo.
Note: If the image does not refresh, it may be due to the browser cache. Reload the page to refresh the image.
3. Click **Save**.

The new branding will now appear on email and reports.

Network Settings

The *Network Settings* section displays:

Configure network settings for this appliance.

IP Address:	10.3.1.184
Subnet Mask:	255.255.255.0
Default Gateway:	10.3.1.1
DNS Server:	8.8.8.8

the appliance's configured DNS/IP settings. Edit these settings should the network configuration change.

Note: Editing the IP address may also require changes at the DNS server. This will be true if any EndPoint uses a host name rather than an IP address to subscribe to the appliance.

Security

ShadowControl supports encrypted communications between endpoints and the ShadowControl appliance. The default certificate provided with the appliance is not recommended for production use. From the Security tab you can upload an SSL certificate issued by a recognized certificate authority.

To install a custom SSL certificate

- From the Security tab, provide the locations to the three required certificate files, then click **Save**.
 - Certificate File
 - Key File
 - Intermediate Bundle File

The ShadowControl appliance uploads the certificate files and restarts its Web server to bring the new certificate online.

Important: ShadowControl uses the Apache Web server, which requires a certificate bundle that contains all three of these files. Because of this, you should use an Apache-supported tool, such as OpenSSL, to generate the certificate bundle. Generating a certificate using Microsoft IIS provides only the Certificate file and will not import successfully into the ShadowControl appliance.

Product Registration

The CMD Product Registration section offers the option to register with StorageCraft. This improves response time if support issues arise.

To complete the registration:

- Enter a primary contact name for the CMD administrator and other details.
- Click **Save**.

Note: This information is used only for supporting CMD.

Subscriptions

An appliance can subscribe to a CMD Portal to scale the system for multiple appliances. A portal provides a single view to monitor all EndPoints on all appliances in the CMD system. Each individual appliance's console however remains available. Administrators at that appliance can then continue to monitor that appliance's specific EndPoints using that console.

Note: These local CMD appliance administrators could be recreated at the portal level and assigned to this appliance's organizations. However, this requires maintaining a second set of credentials for those administrators.

If this appliance is already subscribed to a portal, the Subscriptions section shows the portal's domain name or IP address and port number.

To *subscribe* to a portal:

- Type in the portal's Domain hostname or IP address.
- Accept the default port address (443) or type in the port used by the portal.
- Click **Subscribe**.

This appliance now appears in the portal console. (See [The CMD Portal](#) for more information.)

To *unsubscribe* from the portal, click **Unsubscribe**.

Using the CMD Portal

ShadowControl CMD includes the Portal feature. This feature enables CMD to scale to multiple appliances and thousands of monitored devices. A portal is not, however, a distinct software package. Instead, it is simply another installation of the CMD appliance that other appliances subscribe to. Once one appliance (the source) subscribes to another CMD appliance (the target), the target appliance automatically becomes a Portal. This subscription enables the Portal features on the target appliance. Access to the portal is the same as with other appliances via a browser-enabled console.

This section covers:

- [Understanding the Portal Console](#)
- [Using Org Groups](#)
- [Portal Report Scheduling](#)

- [Defining Portal Settings](#)

EndPoint Summary

The EndPoint Summary lists the total number of subscribed EndPoints. It then breaks down the total by status: *Critical*, *Warning*, and *Unresponsive*.

Total EndPoints	6
■ Critical	0
■ Warning	0
■ Unresponsive	0

Click on a status to display a filtered list of the EndPoints with that status in the Main panel.

Search

The Search function provides a way to filter the list of EndPoints shown in the Main panel.

Note: The Search feature appears only when the Main panel displays the EndPoint List.

To do a search:

1. Enter one or more search terms into the Basic Search box. (Search supports multi-lingual characters.)
2. Click **Search**.

CMD displays a list of any EndPoints that match those search terms in the Main panel.

To search for these terms in only a subset of EndPoints, rather than all the EndPoints on the appliance, click **Advanced Search**. You can then select one or more characteristics of EndPoints such as Name, Organization, Site, Tags, Machine Type, and Status to search in:

X

▼ Advanced Search

Search by

Name
 Organization
 Site
 Tags

Server
 Desktop
 Laptop
 Virtual

Status

Good
 Warning
 Critical
 Offline

After you select the characteristics of the EndPoints you want to search, you can click **Search**. (A search term isn't necessary.) The EndPoint List in the Main panel will change to display only those EndPoints that meet those search criteria.

For example, to display all EndPoints that are servers:

1. Uncheck *Desktop*, *Laptop*, and *Virtual* under Type. Leave *Server* checked.
2. Click **Search**.

The EndPoint List now displays only the servers subscribed to this appliance.

Enter one or more search terms to find matches in the EndPoint list. Click **Search** to display them.

You can also search for EndPoints with various characteristics using Advanced Search. For example, to search for a status list or EndPoints that match a search term, check at least one machine type. Next, check the status you want to view. Click **Search**. CMD displays all EndPoints of the selected machine type that also have the selected status.

Note: You must select at least one machine type when doing an advanced search. Otherwise, the search will fail.

3.2 Main Panel

The CMD console's Main panel can display:

- A Dashboard showing the status of EndPoints and notifications for ShadowProtect, ImageManager, and ShadowControl agent issues.
- A list of all subscribed EndPoints, sorted by status and then by name.
- A specificEndPoint's configuration and status when an EndPoint is selected from the list.
- Various settings pages for the options in the Navigation panel.

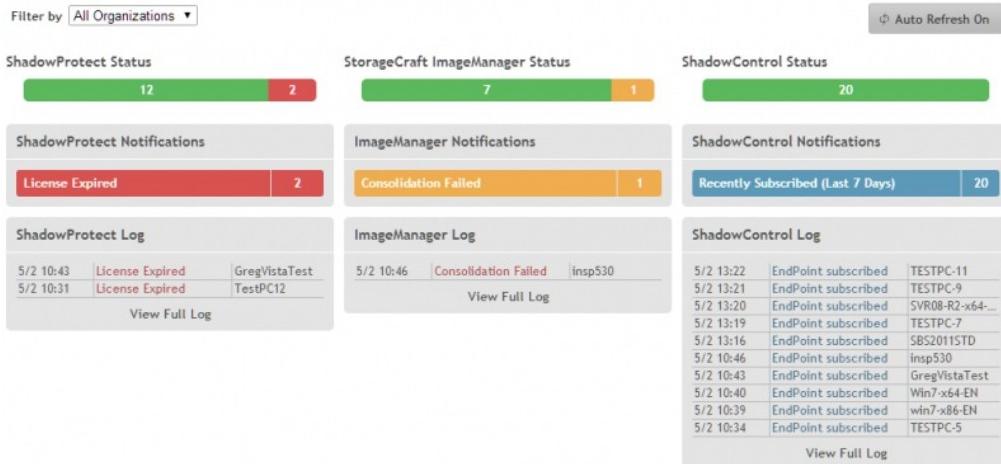
This section discusses the first three:

- Dashboard
- [EndPoint List](#)
- [EndPoint Details](#)

Refer to the [Navigation Panel](#) for details on the settings pages.

Dashboard

The default display in the Main panel is the Dashboard:



The dashboard provides a quick summary of EndPoint status:

- ShadowProtect backup performance
- ImageManager consolidation and replication
- ShadowControl activities with EndPoints

The dashboard can filter the monitored EndPoints displayed by organization using the filter dropdown box at the upper-left. The display automatically updates on a regular basis unless the toggle at the upper-right is set to *Auto Refresh Off*.

EndPoint List

The CMD console can display a list of all subscribed EndPoints on this appliance:

EndPoints				
	EndPoint	Organization : Site	Status	Last Backup
	SBS2011STD	Default Organization	Approval Required: Approve	14 min.
	GregVistaTest	Default Organization	Critical	ShadowProtect license expired.
	TestPC12	Default Organization	Critical	ShadowProtect license expired.
	insp530	Default Organization	Warning	ShadowProtect not installed.
	BIGRED	Default Organization	Good	53 min.
	harris-it-vista	Default Organization	Good	53 min.
	jharris-75	Default Organization	Good	53 min.
	jharris-im	Default Organization	Good	ShadowProtect not installed.
	jharris-LT-2k8r2	Default Organization	Good	3 hours
	jharris-it-8x64	Default Organization	Good	20 min.
	SVR08-R2-x64-EN	Default Organization	Good	ShadowProtect not installed.
	TESTPC_1	Default Organization	Good	8 min.
	TESTPC-11	Default Organization	Good	116 min.
	TESTPC-2	Default Organization	Good	20 min.
	TESTPC-3	Default Organization	Good	17 min.
	TESTPC-5	Default Organization	Good	11 min.
	TESTPC-7	Default Organization	Good	ShadowProtect not installed.
	TESTPC-9	Default Organization	Good	2 min.
	Win7-x64-EN	Default Organization	Good	ShadowProtect not installed.
	win7-x86-EN	Default Organization	Good	ShadowProtect not installed.

The list identifies each with:

Field	Description
Status Icon	Displays the appropriate icon for the device's machine type (server, desktop, laptop, or virtual). Its color represents the EndPoint's current condition (Good, Warning, Critical, Unresponsive).
EndPoint	Displays the name of the device.
Organization:Site	Displays the EndPoint's site and organization as assigned. (If not assigned, it is automatically in the Default Organization.)
Status	Displays the condition of the EndPoint. (If its status is <i>Offline</i> , the field also shows the length of time the EndPoint has been offline.)
Last Backup	Shows the elapsed time since the last backup. If CMD cannot detect this, the field is blank.

Tags

Shows each EndPoint's user defined tag (as assigned in the [EndPoint Details](#) screen).

Results Per Page

The page defaults to show up to 20 EndPoints. Use the selector at the upper-right to increase the number of results from 20 to 50, 75 or 100. If there are more than the selected number of subscribed EndPoints, CMD creates additional pages. The EndPoints appear in order of status then by device name.

Sorting the EndPoint List

Click on a column heading to sort by that column. CMD can sort the EndPoint List by:

Column	Sorting Hierarchy
Name	Alphabetically
Organization	Alphabetically, then each Site is listed alphabetically with EndPoints in each site alphabetically as well.
Status	Lists EndPoints in this order: Unapproved, Offline, Critical, Warning, and Good.
Last Backup	Lists oldest to newest.

Note: The Tags column displays user-defined tags for each EndPoint. Click on a tag to display a new list showing only those EndPoints identified with that tag.

Click on the column title to sort the column. Click on the title again to reverse the order.

Status Icons

Status Icons

The color of the status icon indicates the EndPoint's current condition; its shape indicates the EndPoint's machine type:

Alert Icon	Condition	System Type
	Offline	Server
	Offline	Desktop
	Offline	Laptop
	Offline	Virtual Machine
	Critical	Server

	Critical	Desktop
	Critical	Laptop
	Critical	Virtual Machine
	Warning	Server
	Warning	Desktop
	Warning	Laptop
	Warning	Virtual Machine
	Good	Server
	Good	Desktop
	Good	Laptop
	Good	Virtual Machine

EndPoint Details

Double-click on an individual EndPoint in the EndPoint list to display its details:

Test-Win2012

Info

Status:	Good	Event log...
Platform:	Windows Server 2012 x64	System log...
Processor:	Intel® Dual Band Intel® Dual Band	
Memory:	4.0 GB (18.0% used), 704.0 MB Page file	
Last Restart:	2 days ago	
IP Addresses:	10.2.11.2	
Locale:	en_US Alaskan Daylight Time(UTC-0800)	
Organization:	Servers Edit...	
Site:	None Edit...	
Machine Type:	Server Edit...	
Tags:	- Assign tags...	
Important Applications:		

ShadowProtect

Version:	ShadowProtect 5.0.4.27363(en)					
License:	4231-1245-5643-1234					
Jobs						
Job Name	Status	Last Success	Last Finish Time	Next Run Time	Destination	Actions
unnamed	Queued	17:30, May 1	17:30, May 1	09:30, May 2	VMBackups	

Destinations

Destination	Path
VMBackups	\Test-Host\VM-Backups\VM-Srvr12

Volumes

Listing of all volumes mounted on this EndPoint

Volume	Free Space	Total Space	OS Volume	Protected
System Reserved	52.77 GB	79.66 GB	Yes	No
	108.70 MB	350.00 MB	No	No

ImageManager

Version:	StorageCraft ImageManager 6.5.1.31908(en)
Registered User:	House
Company:	STC
Serial Number:	1234-5678-AAAA-1B34
Managed Folders:	5 Folders Folder Details...

Licensing

License Type	Total	Available	Assigned to Agent	In Use by Agent
ShadowStream Replication Jobs	5	5	0	0
IntelligentFTP Replication Jobs	5	5	0	0
HeadStart Restore Jobs	5	4	1	1
Network Replication Jobs	5	5	0	0

EndPoint Agent Info

Version:	2.0.0.35778
Unsubscribe EndPoint	

EndPoint Details include sections that describe:

- [Info](#)
- [ShadowProtect](#)
- [Volumes](#)
- [ImageManager](#)
- [EndPoint Agent Info](#)

Note: The *EndPoint Details* page supports printer-friendly output for future reference. To print a copy of the EndPoint's details, click on the printer icon in the upper-right corner of the page in the Main panel.

Outstanding Conditions

The Outstanding Conditions section displays the current outstanding conditions for this EndPoint: These conditions occur when the EndPoint exceeds the threshold of one or more of the status rules.

Volume Usage: Exceeded 90% threshold [View details...](#) [Clear status:](#)

- Click **View Details** to view the time and any system message relating to the condition. If the condition has occurred on multiple occasions, CMD will list each of these.
- Use **Clear Status** to either remove this alert immediately or to schedule its removal in 1, 3, or 7 days.

⚠ Note: Using Clear also resets the counter for those rules which keep a cumulative number of events before issuing alerts. For example, non-VSS backups keeps a running total of all non-VSS backups to use with its alert. Click **Clear** to reset this running total.

Info

The Info section displays hardware, operating system, IP address, and other details about the EndPoint.

▼ Info		
Status:	Good	Event log...
Platform:	Windows Server 2012 x64	System log...
Processor:	Intel64 Family 6 Model 58 Stepping 9, GenuineIntel	
Memory:	32.0 GB (56.0% used), 4.3 GB Page file	
Last Restart:	42 days ago	
IP Addresses:	10.2.11.106	
Locale:	en_US Mountain Daylight Time(UTC-0600)	
Organization:	BDR	Edit...
Site:	None	Edit...
Machine Type:	Server	Edit...
Tags:	--	Assign tags...
Important Applications:		

The Info section also provides options for editing various fields. It also has the option to create tags for identifying similar devices using the Search function.

Field	Description	Option
CMD Version	Identifies the installed version of the CMD agent	
Status	Reflects the current condition for the device (Offline, Critical, Warning, Good)	<i>Event Log</i> displays the CMD log (not the Windows System Log) to show the cause of alerts. Acts like the View details option in the Outstanding Conditions section.
Platform	Identifies the operating system version	<i>System Log</i> displays the Windows System Log for the device.
Processor	Identifies the system processor	
Memory	Displays the amount of RAM and page file size	
Last Restart	Gives hours or days since the device restarted	
IP Addresses	Identifies both primary and any subnet addresses	
Locale	Uses the Windows Time Zone data	

Organization	Identifies the device's CMD Organization	Click <i>Edit</i> to display a dropdown box of available CMD organizations
Site	Identifies the site the device is a member of within the current organization shown above	Click <i>Edit</i> to display a dropdown box of available sites within the current CMD organization. It will also offer the <i>Manage Sites</i> option which opens the Sites page.
Machine Importance	Displays critical, semi-critical, or non-critical. The default setting results from CMD best-guess based on the Machine Type.	Click <i>Edit</i> to display a dropdown box for choosing one of the three options.
Machine Type	Shows Server, Desktop, Laptop, or Virtual. The default setting results from CMD analyzing the device to make a best guess as to its type. A correct Machine Type allows CMD to accurately monitor and report conditions.	Click <i>Edit</i> to display a dropdown box for choosing one of the four options.
Tags	Displays any user-defined tags applied to this device. Tags simplify locating specific EndPoints based on a common characteristic or role.	Click <i>Assign tags</i> to open the list of defined tags and select one or more for this EndPoint. The list includes the option to create more. Note: Tags support multi-lingual characters.
Important Applications	Displays a list of critical applications running on this device. CMD performs a check to automatically identify these which include <i>SQLServer</i> , <i>IIS</i> , and <i>Microsoft Exchange</i> .	

ShadowProtect

The ShadowProtect section displays the version number and license status of the ShadowProtect install on the EndPoint. It also displays details of current backup jobs and their destinations.

ShadowProtect						
Version:	ShadowProtect 5.0.4.27363(en)					
License:	4231-1245-5643-1234					
Jobs						
Job Name	Status	Last Success	Last Finish Time	Next Run Time	Destination	Actions
unnamed	Queued	17:30, May. 1	17:30, May. 1	09:30, May. 2	VMBackups	
Destinations						
Destination	Path					
VMBackups	\Test-Host\VM-Backups\VM-Srvr12					

Note: CMD will show the message "ShadowProtect is not installed on this EndPoint" if that is the case.

Activate ShadowProtect Licensing

CMD will not only detect if ShadowProtect is installed, but also if it is in Trial mode or if its license has expired. In either case, CMD will display the **Activate** button:

ShadowProtect	
Version:	ShadowProtect 4.2.7.19756 (en)
License:	License Expired. 

Click **Activate** to enter the license number:

FDAG-2 - Activate ShadowProtect

Enter your licensing information to remotely activate ShadowProtect.

Serial Number:	<input type="text"/>
Customer Name (Optional):	<input type="text"/>
<input type="button" value="Cancel"/>	<input type="button" value="Activate"/>

1. You must enter a valid license number.
2. Enter a customer name to simplify referencing this ShadowProtect when working with StorageCraft Support.
3. Click Activate to push the license to this EndPoint.
4. The EndPoint Details screen will update with the new license number.

Note: This license number push install only works with ShadowProtect version 4.2.5 and newer.

Backup Jobs

The ShadowProtect section offers options to see further information about the job or destination:

Field	Description	Option
Jobs	Identifies details for all ShadowProtect backup jobs defined for this device	Click <i>Actions</i> to show the job's last run time, next runtime, results, and the last backup job's event log.

Destinations	<p>Displays details on the configured backup file destinations for this device.</p> <p>Some destinations require credentials to access them. For this reason, some destination backup file lists may show no entries.</p>	<p>Click <i>Backup Images</i> to display a list of the backup files stored on the selected destination. This list will also show date and time of each file, its name, type, size, and other details.</p>
---------------------	---	---

Volumes

The Volumes section displays details on all volumes mounted on the EndPoint.

▼ Volumes					
Listing of all volumes mounted on this EndPoint					
Volume	Free Space	Total Space	OS Volume	Protected	
My Passport	31 GB	931 GB	No	No	More details...
OS	248 GB	297 GB	Yes	Yes	More details...
RECOVERY	523 MB	751 MB	No	No	More details...

These volume details include:

Field	Description
Volume	Displays the volume label for all partitions on each accessible drive to the device. Note: This list might display hidden volumes.
OS Volume	Indicates whether this is a boot volume.
Protected	Indicates whether ShadowProtect performs backups of this partition.
<i>More details</i>	<p>Displays a list including:</p> <ul style="list-style-type: none"> • the mount point • free/total space • sector/cluster size • if ShadowProtect backs up this partition

ImageManager

This section displays the ImageManager licensing details for this EndPoint.

Note: CMD displays a message if ImageManager is not installed. If ImageManager is installed but not registered, CMD will only show the version number .

▼ ImageManager

Version: StorageCraft ImageManager 6.5.1.31908(en)
 Registered User: House
 Company: STC
 Serial Number: 1234-5678-AAAA-1B34
 Managed Folders: 5 Folders [Folder Details...](#)

Licensing

License Type	Total	Available	Assigned to Agent	In Use by Agent
ShadowStream Replication Jobs	5	5	0	0
intelligentFTP Replication Jobs	5	5	0	0
HeadStart Restore Jobs	5	4	1	1
Network Replication Jobs	5	5	0	0

If one or more of ImageManager's premium features are installed, CMD will show:

- The number of licenses for each type of premium feature.
- The number of assigned vs. available licenses.
- If any premium feature license is expired

(Refer to the [ShadowControl ImageManager User Guide](#) for details on these premium features.)

Unlicensed Versions of ImageManager

If the endpoint has an unlicensed version of ImageManager prior to 6.0, CMD only displays the unlicensed status, not the version number:

▼ ImageManager

Version: 0.0.0(en-US) ImageManager (unlicensed)
 Registered User: --
 Company: --
 Serial Number: --

If the unlicensed version is newer than 6.0, CMD displays the version number as well as the unlicensed status.

EndPoint Agent Info

The EndPoint Agent Info section displays the version number of the installed CMD agent. It also provides the option to unsubscribe the EndPoint from this appliance.

To unsubscribe from an appliance

1. Click **Unsubscribe EndPoint**.
2. CMD asks to confirm this action.

Once the EndPoint unsubscribes to the appliance, CMD will no longer monitor that EndPoint.

3.3 Session Panel

The Session Panel appears at the top right of the console:



This panel displays:

- User** Shows the currently logged-in username.

Account Settings

Displays in the Main panel the currently logged-in user's settings. The user can then change their password, email address, the type of notifications to receive (All, Critical Only, or None), or the user's preferred language. Click **Save** to save the new settings. (Use the *Appliance Accounts* option in the Navigation panel to change the administrative role if needed.)

Help

Opens a new tab in the browser to display this *ShadowControl CMD User Guide*. (Requires Internet access.)

Logout

Logs out the user out of the appliance console

Appliance Identifier

Shows the name of this appliance. This identification is useful for managing multiple CMD appliance systems.

4 Using Status Rule Policies

Status Rules Policies are the heart of CMD's monitoring. All EndPoints use the Default Policy unless assigned to a specific new policy:

ShadowControl Status Rule Policy

Policy Name:

ShadowControl Rules

EndPoint Unresponsive - Trigger an alert if the EndPoint has not communicated with the appliance within the specified time period.
 Minutes Alert using Severity:

ShadowProtect Rules

Failed Backup Job - Trigger an alert if the backup job remains in a failed state for the specified time period.
 Hours Alert using Severity:

Backup Failure Rate - Trigger an alert if the endpoint exceeds the specified ratio of backup failures to backup attempts.
 Backup failures: Compared to total backups: Alert using Severity:

Last VSS Backup - Trigger an alert if no successful VSS backup occurs within the specified time period.
 Days Alert using Severity:

Destination Disk Usage - Trigger an alert if a destination's disk usage exceeds the specified percentage.
 Warning Alert level: Critical Alert level:

License Status - Trigger a warning alert when a ShadowProtect MSP license is 5 days from expiration. Trigger a critical alert when a license expires.

Service Status - Trigger an alert if the ShadowProtect service becomes unresponsive.

ImageManager Rules

Managed Folder Disk Usage - Trigger an alert if a managed folder's disk usage exceeds the specified percentage.
 Warning Alert level: Critical Alert level:

Verification Status - Trigger an alert if an ImageManager verification job fails.

Consolidation Status - Trigger an alert if an ImageManager consolidation job fails.

Replication Queue Size - Trigger an alert if a replication job's queue exceeds the specified number of files.
 Maximum: Alert using Severity:

License Status - Trigger a warning alert when an ImageManager MSP license is 5 days from expiration. Trigger a critical alert when a license expires.

Service Status - Trigger an alert if the ImageManager service becomes unresponsive.

Note: By default, various status rules are active with thresholds set based on best practice. Administrators can select which rules to apply to a given organization or site.

Severity and Status Icons

Most of the rules include a setting for severity: *Warning* or *Critical*. CMD uses the severity setting as the threshold to change the icon shown for the affected EndPoint in the EndPoint list as well as issue notifications. An administrator can select this severity setting based on their requirements or concerns for their EndPoints.

For example, an administrator may create a unique set of status rules for a Policy called "Servers" then add all server EndPoints to use this policy.

EndPoint-Based Rules

ShadowControl is an EndPoint-focused monitoring tool. This means that it issues alerts for a change of state for each EndPoint, not for each threshold exceeded. For example, if the EndPoint's ImageManager encounters two or more backup file verification errors, ShadowControl reports the first occurrence not subsequent ones. The date of this first occurrence appears in the logs and is not updated for subsequent errors.

4.1 ShadowControl Rules

The Status Rule Policy for ShadowControl includes:

Rule	Description	Active by Default?	Default Value	Rule Options	Severity Options
EndPoint Unresponsive	When checked, CMD issues an alert when an EndPoint has not communicated with the appliance within the specified time period.	Yes	15	Minutes (Default), Hours, Days	Critical (Default), Warning

4.2 ShadowProtect Rules

The Status Rule Policy for ShadowProtect includes:

Rule	Description	Active by default?	Default Value	Rule Options	Severity Options
Failed Backup Job	When checked, triggers an alert if the EndPoint has not communicated with the appliance within the specified time period.	Yes	1 Hour	Minutes, Hours (Default), Days	Critical (Default), Warning
Backup Failure Rate	When checked, triggers an alert if the endpoint exceeds the specified ratio of backup failures to backup attempts. This rule works if a backup failure occurs not just once, but on multiple occasions within a set number of backups. This rule escalates the alert that the Failed Backup Job rule generates by notifying the administrator that a pattern of failures is occurring (in other words, when the failures are not consecutive).	No	3 failures in the last 5 backup attempts	Number of backup failures, Number of total backups	Critical (Default), Warning
Last VSS Backup	ShadowProtect leverages Windows VSS support to provide optimal backups for server applications such as SQL or Exchange. If a problem occurs with VSS (such as with an unreliable third-party VSS writer), ShadowProtect may resort to performing a "crash-consistent" non-VSS backup. A "crash-consistent" backup may require additional recovery effort, so CMD issues an alert whenever the set period of time passes without a VSS backup.	No	1 Day	Minutes, Hours, Days (Default)	Critical (Default), Warning

Destination Disk Usage	When checked, CMD issues an alert whenever the amount of used space in the image file destination drive exceeds the specified threshold.	Yes	90% usage for Warning, 95% for Critical	Warning percentage, Critical percentage	Critical (Default), Warning
License Status	When checked, CMD issues a Warning alert when a system using a ShadowProtect MSP license is 5 days from expiration. It issues a Critical alert when the MSP license expires.	Yes	N/A	None	None
Service Status	When checked, CMD issues an alert if the ShadowProtect service is not responding.	Yes	N/A	None	Warning (Default), Critical

4.3 ImageManager Status Rules

The Status Rule Policy for ImageManager includes:

Rule	Description	Active by Default?	Default Value	Rule Options	Severity Options
Managed Folder Disk Usage	When checked, CMD issues an alert if the used space on the drive with the managed folders exceeds the set threshold.	Yes	Warning: 90% Critical 95%	Specify the percent of disk space used	N/A
Verification Status	When checked, CMD issues an alert if an image file fails its verification test. (This test confirms the fidelity of the file for restoration.)	Yes	Critical	Severity level	Critical, Warning
Consolidation Status	When checked, CMD issues an alert if an ImageManager consolidation job fails.	Yes	Critical	Minutes, Hours, Days	Critical, Warning
Replication Queue Status	When checked, CMD issues an alert when the list of files waiting to replicate exceeds the specified threshold. (This could indicate a failed network connection or destination server.)	Yes	20 files	Specify the maximum number of files in the queue	Warning (Default), Critical
License Status	When checked, CMD issues a Warning alert when a system with an ImageManager MSP subscription is 5 days from the license expiration. It issues a Critical alert when the MSP license expires.	Yes	N/A	N/A	N/A
Service Status	When checked, CMD issues an alert if the ImageManager service has not responded in the last five minutes.	Yes	Warning	Severity level	Warning (Default), Critical

4.4 Status Rules Details

Each CMD status rule has specific thresholds and scope:

Backup File Size

This alert provides notice that a ShadowProtect backup image file exceeded a user-defined threshold. This alert might safeguard against running out of storage space on the backup drive or it might indicate an unusual amount of activity on the source device that warrants investigation. This alert displays (until cleared) even when subsequent backup files may not exceed the set threshold.

To clear an alert:

1. Locate the EndPoint's Backup File Size alert in the *Outstanding Conditions* section of the EndPoint Details page.
2. Click **Clear** to immediately remove the alert. (CMD also supports scheduling this clearing at a later time using the dropdown box.)

Non-VSS Backup

ShadowProtect leverages Windows VSS support to provide optimal backups for server applications such as SQL or Exchange. If a problem occurs with VSS (such as with an unreliable third-party VSS writer), ShadowProtect may resort to performing a "crash-consistent" backup. A "crash-consistent" backup may require additional recovery effort, so by default CMD will issue an alert whenever a non-VSS backup occurs.

Note: Some EndPoints may not support VSS. Refer to [Installing the CMD Agent](#) for details on avoiding multiple alerts due to non-VSS support on an EndPoint.

The non-VSS backup counter is cumulative, not consecutive. If the affected system has a status rule for non-VSS backups with a value of "2", then if it suffers one non-VSS backup, then a successful VSS backup, then another non-VSS backup, CMD issues an alert. CMD also issues an alert if the system suffers from two consecutive non-VSS backups. (Use the EndPoint Details screen to clear this counter.)

ImageManager Status

This CMD alert activates when ImageManager issues an error. Refer to the [ImageManager console](#) for details on the type of error and how to resolve it.

Backup Consistency

This rule works in conjunction with the **Backup Failure** rule. This consistency rule generates an alert if a backup failure occurs not just once, but on multiple occasions within a set number of backups. In essence, Backup Consistency escalates the alert that the Backup Failure rule generates by notifying the administrator that a pattern of failures is occurring (in other words, when the failures are not consecutive).

Backup Failure

This rule generates an alert if there is a single backup failure (if the setting is "1"). If the number is set to "2" or more, it generates an alert only after the set number of failures occur in a row, rather than separately.

Services

The Services rule applies to various monitored Windows services, including the ShadowProtect and ImageManager services. If Windows logs an issue with any of the monitored services, CMD will display a Services alert. View details of the particular Services alert in the Windows System Log.

RAM Usage

This rule alerts administrators to possible backup issues should the EndPoint exhaust available RAM.

Storage System Errors

This rule alerts administrators to storage or file system events as shown in the Windows System log. CMD issues an alert when the number of such events exceeds the defined threshold.

Volume Usage

Alerts administrators that a protected volume may run out of available space.

Machine Offline Status Rules

CMD will alert administrators if an EndPoint goes offline and after how long. This Machine Offline status rule can apply based on machine importance.

Note: Each EndPoint has a user-definable *Machine Importance* setting on its [EndPoint Details](#) page. These settings are *Non-critical*, *Semi-critical*, and *Critical*. (CMD assigns a default setting of non-critical to all subscribed EndPoints.)

Administrators should determine which EndPoints represent a more significant part of their operations and set an appropriate machine importance to them. For example, all servers may have a Critical machine importance setting. Desktops in "Accounting" may have Semi-Critical or Critical importance. Personal systems may have a Semi-Critical or Non-Critical setting.

The Offline rules have two levels of alert--Critical and Warning--and also include an elapsed time setting. This setting specifies the number of minutes, hours, or days for the system to be offline before CMD issues a Warning or Critical alert.

5 Reporting

The Reports option in the Navigation panel displays report settings and a list of recent archived reports in the Main panel:

The screenshot shows the 'Reports' section of the ShadowControl CMD interface. It includes a 'View Report' button (disabled), a 'Schedule Reports' button, and a 'Recently Generated Reports' section. The 'Recently Generated Reports' section lists reports from 'SuperAdmin Reports' and 'Administrator Reports' for 'shadowcontrol-appl1' on May 01, 2014. It also shows 'Organization Reports' for 'BDR', 'Desktops', and 'Servers' on the same date. Below this is an 'Additional Information' section for 'ShadowProtect Licensing'.

Organization / Admin	Date
SuperAdmin Reports	May 01, 2014
shadowcontrol-appl1	May 01, 2014
Administrator Reports	No reports have been sent.
Organization Reports	
BDR	May 01, 2014
Desktops	May 01, 2014
Servers	May 01, 2014

This screen has four elements:

Element	Description
View Report	Click this button to view the latest superadmin report in a new browser tab. (See the Sample Report for further details.)
Schedule Reports	Click this button to view the report scheduling page (See Report Scheduling for details.)
Recently Generated Reports	This section lists recently archived reports. (CMD only keeps a rolling 30-day record.) Click on a report in the list to view it in HTML in a new browser tab.
Additional Information	This section provides further information that is not included in the standard reports. It includes an on-demand report showing ShadowProtect license usage. (For details, see ShadowProtect Licensing .)

Note: Reports are sent to users in the language selected in the user's *Preferred Language* setting.

5.1 Report Scheduling

The **Schedule Reports** button on the Reports page displays the *Report Scheduling* settings page:

Report Scheduling

Schedule the generation of reports tailored to specific administrators and contacts. Reports are sent by email according to the selected schedule.

SuperAdmin Report

Send a report to each SuperAdmin	Send reports: Every day
Report will contain a Summary section and any of the following sections: <input checked="" type="checkbox"/> EndPoint Connectivity: overall connection status of all monitored EndPoints <input checked="" type="checkbox"/> EndPoint Backup: listing of last backup for each ShadowProtect installation <input checked="" type="checkbox"/> Storage: summary of storage space used by backups <input checked="" type="checkbox"/> Backup Details: last backup and backup summary information for each endpoint site	

Administrator Report

Send an organization report to each Administrator	Send reports: Every week
Report will contain a Summary section and any of the following sections: <input checked="" type="checkbox"/> EndPoint Connectivity: overall connection status of all monitored EndPoints <input checked="" type="checkbox"/> EndPoint Backup: listing of last backup for each ShadowProtect installation <input checked="" type="checkbox"/> Storage: summary of storage space used by backups	

Organization Report

Send an organization report to the primary contact of each organization	Send reports: Every month
Report will contain a Summary section and any of the following sections: <input checked="" type="checkbox"/> EndPoint Connectivity: overall connection status of all monitored EndPoints <input checked="" type="checkbox"/> EndPoint Backup: listing of last backup for each ShadowProtect installation <input checked="" type="checkbox"/> Storage: summary of storage space used by backups <input checked="" type="checkbox"/> Backup Details: last backup and backup summary information for each endpoint site	

[Save Schedule](#) [Cancel](#)

To send a report:

1. Select the Type, Frequency, and Role of the report. The defaults send a complete report every day to SuperAdmin and Administrators as well as the primary contact for each organization.
2. Click **Save Schedule**.
3. CMD issues reports based on the options selected.

Types of Reports

The scheduler generates a report with four possible sections based on the selected options:

Summary Displays a chart of EndPoint status (Critical, Warning, Good or Offline), a list of the backup success rate for the report's time period, and a list of ShadowProtect/ImageManager installations and platforms.

EndPoint Backup Displays a list of the EndPoints by organization, their backup success rate for the report's time period, and when their last backup occurred.

Displays a list of the EndPoints by organization with their:

EndPoint Status

- Length of time CMD actively monitored the EndPoint
- Average number of times per day the EndPoint is offline
- Operating system version details.

Storage Summary Displays a set of daily averages for the amount of disk space used by backup image files. CMD uses this data to create a chart of projected storage space requirements for the next 3, 6, and 12 months.
Note: This is only a rough estimate and varies based on the rate of change of data in each backup.

Backup Details Displays the last backup information for each EndPoint.

Specific Role Reports

CMD can send a report to a specific role. Each role receives a report covering a different set of EndPoints:

SuperAdmin This report covers all EndPoints on this appliance.

Administrator	This report shows only those EndPoints in organizations assigned to each administrator. The report does not include last backup details.
Organization	This report (sent to an organization's primary contact) lists only the EndPoints in that organization.

Frequency

CMD can then send these reports on a selected schedule:

Never	CMD sends no reports.
Every Day	CMD sends a summary report of the last 24 hours once a day.
Every Week	CMD sends a summary report of the last 7 days once a week.
Every Month	CMD sends a summary report for the last 30 days once a month.

5.2 Sample Report

CMD reports can have four sections:

EndPoint Summary	Displays a chart of the number of EndPoints that are Critical, Warning, Good or Unresponsive and a list of ShadowProtect, ImageManager, and ShadowControl agent notifications.
-------------------------	--

ShadowProtect EndPoint Details	Lists the EndPoints by organization, their backup job success summary for the report's time period, the size of the EndPoint's last backup file and the average size for these files per day, and the EndPoint status.
---------------------------------------	--

Note: Supports ShadowProtect v4.2.7 and newer.

ImageManager EndPoint Details	<p>Lists the EndPoints by organization with their:</p> <ul style="list-style-type: none"> • ImageManager job status (including replication and HSR) • Number of replication and HSR licenses • Managed Folder summary (number of managed folders, number of images, and total disk space used) • Current EndPoint status
--------------------------------------	--

Note: Requires ImageManager 6 or newer.

Storage Statistics	<p>Displays a set of daily averages for the amount of disk space used by backup image files. CMD uses this data to create a chart of projected storage space requirements for the next 3, 6, and 12 months.</p> <p>Note: This is only a rough estimate. It varies based on the rate of change of data in each backup.</p>
---------------------------	--

A sample report showing all four sections appears like this:



ShadowControl Appliance Daily Report: shadowcontrol-appl1					
Endpoint Summary		ShadowProtect Status			
 ShadowProtect Notifications No status notifications		 StorageCraft ImageManager Status No status notifications			
 ShadowControl Status Recently Selected Last 7 Days					
ShadowProtect Endpoint Details					
Desktops					
Endpoint Backup Job Summary		Storage Summary Average job size: 1.04 GB Average per day: 1.16 MB			
1 backup job initiated. Last backup at 7/29/2011 01:10:00 AM (incremental). 1 backup job completed. 1 backup job succeeded. 10 backup jobs initiated. 10 backup jobs completed. 10 backup jobs succeeded.		 Status: OK			
Endpoint Backup Job Summary		Storage Summary Average job size: 1.04 GB Average per day: 1.16 MB			
1 backup job initiated. Last backup at 7/29/2011 01:10:00 AM (incremental). 1 backup job completed. 1 backup job succeeded.		 Status: OK			
Endpoint Backup Job Summary		Storage Summary Average job size: 1.04 GB Average per day: 1.16 MB			
1 backup job initiated. Last backup at 7/29/2011 01:10:00 AM (incremental). 1 backup job completed. 1 backup job succeeded.		 Status: OK			
Servers					
Endpoint Backup Job Summary		Storage Summary Average job size: 1.04 GB Average per day: 1.16 MB			
1 backup job initiated. Last backup at 7/29/2011 01:10:00 AM (incremental). 10 backups total of 11 succeeded.		 Status: OK			
1 backup job initiated. Last backup at 7/29/2011 01:10:00 AM (incremental). 10 backups total of 11 succeeded.		 Status: OK			
BCR					
Endpoint Backup Job Summary		Storage Summary Average job size: 1.04 GB Average per day: 1.16 MB			
No backup jobs received.		 Status: OK			
ImageManager Endpoint Details					
Desktops					
Endpoint Job Summary		Folder Summary			
 Status: OK		 Status: OK			
<small>There are no endpoints with ImageManager installed.</small>					
Servers					
Endpoint Job Summary		Folder Summary			
 Status: OK		 Status: OK			
<small>There are no endpoints with ImageManager installed.</small>					
BCR					
Endpoint Job Summary		Folder Summary			
 Status: OK		 Status: OK			
Storage Statistics					
Desktops					
<small>Size of stored backup images from all endpoints</small>					
Average Daily Image Usage: Per Endpoint: 1.1 GB Entire Organization: 41.1 MB		Accidental Storage Forecast (based on recent usage): 3 Months: 3.94 TB 6 Months: 7.88 TB 12 Months: 15.76 TB			
					
Servers					
<small>Size of stored backup images from all endpoints</small>					
Average Daily Image Usage: Per Endpoint: 1.1 GB Entire Organization: 41.1 MB		Accidental Storage Forecast (based on recent usage): 3 Months: 10.5 GB 6 Months: 21.0 GB 12 Months: 42.0 GB			
					

5.3 ShadowProtect Licensing

The **Additional Information** section under Reports can display ShadowProtect license usage for EndPoints subscribed to this appliance. Click **ShadowProtect Licensing** to display this report:

ShadowProtect Licensing	
Americas	
License	EndPoint
6.1.7606	test-420-027
None	test-425-030
APAC	
License	EndPoint
6.1.7601	vm2000sv-en
6.1.7607	test-420-001
EMEA	
License	EndPoint
None	CMD-EP-2008-1
None	LAP-W7-DaD

CMD orders these details by organization.

Note: Accurate licensing reports requires ShadowProtect v4.2.7 or newer on the EndPoint.

6 Upgrading CMD

CMD includes an automated system to upgrade the appliance and EndPoints to the latest software version. The *System Info* section of the Appliance Settings screen will show an **Update Appliance** button when CMD detects a new version available for download:



1. Click **Release Notes** to review new features or enhancements of the upgrade. Online, refer to the [CMD ReadMe](#) file.
 2. Click **Update Appliance**.
 3. The wizard displays scheduling options for the appliance and for EndPoints:

System Info	
Version	ShadowControl v1.1.15.24247 [1.7-24247, 22] Release Notes
<input style="background-color: #e0e0e0; border: 1px solid #ccc; padding: 2px 10px; width: 150px; height: 25px;" type="button" value="Update Appliance"/>	
<input style="background-color: #e0e0e0; border: 1px solid #ccc; padding: 2px 10px; width: 150px; height: 25px;" type="button" value="Schedule Update"/>	
Schedule Appliance Update: <input style="border: none; padding: 0; margin-right: 10px;" type="button" value="Start immediately"/> <input style="border: none; padding: 0;" type="button" value="?"/>	
EndPoint Update Window: <input style="border: none; padding: 0; margin-right: 10px;" type="button" value="15 minutes"/> <input style="border: none; padding: 0;" type="button" value="?"/>	
<input style="background-color: #e0e0e0; border: 1px solid #ccc; padding: 2px 10px; width: 150px; height: 25px;" type="button" value="Set Timezone"/>	
<input style="background-color: #e0e0e0; border: 1px solid #ccc; padding: 2px 10px; width: 150px; height: 25px;" type="button" value="Reboot Appliance"/> <input style="background-color: #e0e0e0; border: 1px solid #ccc; padding: 2px 10px; width: 150px; height: 25px;" type="button" value="Shut Down Appliance"/>	
Access Code: func0 RAM Usage: 540 MB of 995 MB available (45.7% used) Disk Usage: 12 GB of 14 GB available (14.3% used) CPU Usage: 0.00 Load Average (5 min.): 0.42	
Appliance Timezone: <input style="border: none; padding: 0;" type="button" value="America/Monterrey"/> <input style="border: none; padding: 0;" type="button" value="America/Montevideo"/> <input style="border: none; padding: 0;" type="button" value="America/Montreal"/> <input style="border: none; padding: 0;" type="button" value="America/Montserrat"/> <input style="border: none; padding: 0;" type="button" value="America/Nassau"/> <input style="border: none; padding: 0; background-color: #0070C0; color: white;" type="button" value="America/New_York"/>	

Select a time to update the appliance.

4. Select a time when CMD should complete the updates to EndPoint agents. CMD will randomly update each EndPoint during that interval to conserve bandwidth.
5. Click **Schedule Update**. CMD will install the latest software on the appliance. It will then automatically push the latest client software to each EndPoint and install it. **Note:** Automatic updating requires EndPoint agent v2.0.0 or newer installed.
6. Export a backup of the Appliance database. Click **Appliance Settings > Appliance Backup > Export Backup File**.

⚠ No reboot is necessary at the EndPoints after an upgrade. In rare cases, anEndPoint may lose contact with the CMD appliance if the appliance was reinstalled during an upgrade. If this occurs, open a command prompt as administrator. Use the `stccmd unsubscribe -F` command found in the Program Files (x86)\StorageCraft\cmd directory to force a change in subscription. Use the `stccmd subscribe ipaddress` command with the appliance's IP address to renew the connection.

Manual Updates for EndPoints

Push Updates for EndPoints only works for CMD agent versions 1.1.1 to 1.3. Upgrades from older agents to 2.0 require manual updating.

To perform a manual update:

1. Download the latest agent from [the Support page](#).
2. Copy, unzip, and run the client install on each EndPoint.

The update will retain the previous version's appliance subscription and settings.

⚠ Warning: Push updates will not work for Windows 2000 EndPoints as CMD v1.1.1 and newer does not support Win2K EndPoints. Previous CMD client software for Windows 2000 will also not interoperate with CMD v1.1.1 or newer appliances. As an alternative for Win2K EndPoints, uninstall the old CMD client and use the ShadowProtect console's management tools to monitor these EndPoints.

Slow EndPoint Updates

EndPoint updates consume network bandwidth. Depending on the number of EndPoints, updates could consume all available bandwidth as EndPoints continually try to resume a failed update. To avoid this, stage updates over a period of time.

In smaller systems, an EndPoint auto-update may still not complete immediately. StorageCraft recommends waiting an interval of time for the EndPoint to update prior to performing one of the alternative update strategies below. On rare occasions, the EndPoint automatic update process may fail. If this occurs:

1. Select the affected EndPoint in CMD's EndPoint list. This should trigger the automatic update process.
2. If this should fail to update the EndPoint, click **Update Now** in the EndPoint Details Agent info field. This also triggers the automatic update process.
3. If neither of these initiate the update, restart the StorageCraft Endpoint Agent service in the affected system's Windows Services tool. Then use the CMD console to perform Steps 1 or 2. Again, the update process may take some time.
4. If these don't initiate the automatic update, perform a manual install of the EndPoint agent on the affected system.

7 CMD Backup and Restore

The ShadowControl CMD appliance maintains a database of subscribed endpoints and their backup history. StorageCraft recommends making a copy of this database at least weekly (and especially after an upgrade) as a precaution against a system failure. While rebuilding a failed appliance is not difficult, resubscribing multiple endpoints and retrieving their data can become an extended process--particularly on sites with over a hundred endpoints.

To Backup the CMD Appliance

1. In ShadowControl, select **Appliance Settings > Appliance Backup > Export Backup File**.
Caution: The export process may take a few minutes. Do not press <F5> to refresh the screen to try and view the current progress of the export. Pressing <F5> causes ShadowControl to abandon the first export and initiate a new one. This prolongs the export process.
Once the export completes, ShadowControl displays the location and date/time stamp of the exported database file.
2. Right-click on the file name and click **Save Link As**.
3. Select an external destination for the backup database file.
4. Click **Save**. ShadowControl saves a copy of the file to the destination.
5. The CMD database does not include customized branding graphics. Create a separate copy of these another drive to reinstall these after a CMD restore.
6. The database also does not include network settings or custom SSL certificates. Again, keep a separate copy of these for reference during the restore.

To Restore the CMD Appliance

1. On new or restored hardware, confirm access to the external or network drive with the CMD database backup file.
2. Rerun the ShadowControl install program. The *Initial Appliance Setup* dialog displays a choice of configuration options:



3. Select *Restore this appliance from a ShadowControl database backup file*.
4. Click **Browse** to locate and select the backup file.
5. Click **Save**. The setup program restores the appliance's configuration.
Note: No access code is required to do this restore.
6. Manually reconfigure the appliance's time zone, network settings, and custom SSL certificates. Reconfigure any branding graphics.

Follow the remaining steps in the setup wizard to complete the restore.

8 Appendix: Using the CMD Portal

ShadowControl CMD includes the Portal feature. This feature enables CMD to scale to multiple appliances and thousands of monitored devices. A portal is not, however, a distinct software package. Instead, it is simply another installation of the CMD appliance that other appliances subscribe to. Once one appliance (the source) subscribes to another CMD appliance (the target), the target appliance automatically becomes a Portal. This subscription enables the Portal features on the target appliance. Access to the portal is the same as with other appliances via a browser-enabled console.

This section covers:

- [Understanding the Portal Console](#)
- [Using Org Groups](#)
- [Portal Report Scheduling](#)
- [Defining Portal Settings](#)

8.1 Understanding the Portal Console

The Portal console provides configuration controls and displays the status of all EndPoints on all subscribed appliances:

Endpoint	Appliance	Organization : Site	Status	Last Backup	Tags
Vista-x86-EN	VirtualAppliance	Default Organization	Approval Required	5 min.	--
WIN-QDOVCA6R8QI	VirtualAppliance	1stOrgGroup	Offline (8 hours)	--	--
Vm-win7-PC	VirtualAppliance	1stOrgGroup	Critical	--	--
vmxpipro-x64-EN	VirtualAppliance	1stOrgGroup	Critical	6 min.	--
wm7-x86-EN	VirtualAppliance	1stOrgGroup : VirtualSite	Critical	--	--
vm2000pro-en	VirtualAppliance	1stOrgGroup : 2000VovVSS	Warning	--	--
vmsbs-2003-en	VirtualAppliance	1stOrgGroup : 2000VovVSS	Good	6 min.	--
VM-Win7x64-PC	VirtualAppliance	1stOrgGroup : VirtualSite	Good	6 min.	--
Wln7-x64-De	VirtualAppliance	1stOrgGroup : VirtualSite	Good	6 min.	--

The Portal console is divided into three panels:

Navigation Panel: Located at the left side of the console, the Navigation panel provides access to the tasks and tools necessary to configure and monitor EndPoints. For more information, see the CMD console [Navigation Panel](#) section.

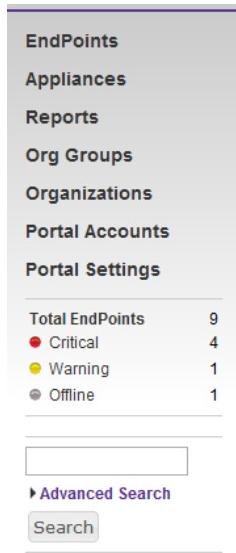
Main Panel: Located at the center of the console, the Main panel displays various lists or configuration settings depending on the option selected in the Navigation panel. (The default is to display a list of all EndPoints the Portal monitors.) For details, see the

CMD console [Main Panel](#) section.

Session Panel: Located at the top of the console, the Session panel displays the Portal indicator, the name of the currently logged-in user, and options for account settings, Help, and Logout. For more information, see the CMD console [Session Panel](#) section.

Portal Navigation Panel

The left-side Navigation Panel provides access to the Portal's tasks, EndPoint summary, and Search capability:



Total EndPoints	9
● Critical	4
● Warning	1
● Offline	1

[Advanced Search](#)

[Search](#)

The selections include:

EndPoints: Displays a list of all the EndPoints on all subscribed appliances in the Main panel.

Note: Use the *Search* feature to filter the list.

Appliances: Displays the list of subscribed appliances in the Main panel. Click on an appliance to display a subset of its configuration settings. These include Organizations, Sites, User Accounts, and Email settings. It also presents options to **Unsubscribe** or **Reboot** the appliance. See [Understanding the CMD Console](#) for further details.

Reports: Displays the Report Scheduling settings. Use this to configure reporting (see [Portal Report Scheduling](#) for details).

Org Groups: Displays the list of defined Org Groups for this portal. See [Using Org Groups](#) for details.

Organizations: Displays a list of Organizations from all subscribed appliances. Use this screen to assign the Organizations to Org Groups. See [Using Org Groups](#) for details.

Sorting the Portal's Organization List

CMD can sort a Portal's Organization List by clicking on the relevant header. (Since this list includes every organization from every appliance monitored by the portal, it can become quite large.) The header includes:

Column	Sorting Hierarchy
Organization	Alphabetically by name
Appliance	Alphabetically by name, then by organization name alphabetically

Portal Accounts: Displays the list of defined accounts for this Portal. See [Defining Portal Settings](#) for details.

Portal Settings: Displays the various email and network settings for this portal. See [Defining Portal Settings](#) for details.

EndPoint Summary: Displays the total number of EndPoints that report to this portal. It also shows the number of EndPoints in Offline, Warning, or Critical Status. Click on the status to display a filtered list of the EndPoints with a specific status in the Main panel.

Search: Type in a search term to display a list of EndPoints, organizations, or sites that include the term.. See [Search](#) for more information.

Portal Main Panel

The Portal Main panel by default shows a list of all EndPoints on all subscribed appliances:

EndPoints					
EndPoint	Appliance	Organization : Site	Status	Last Backup	Tags
Vista-x64-EN	VirtualAppliance	Default Organization	Approval Required	5 min.	--
WIN-QDOVCA6R8QI	VirtualAppliance	1stOrgGroup	Offline (8 hours)	--	
Vm-win7-PC	VirtualAppliance	1stOrgGroup	Critical	--	
vmxppro-x64-EN	VirtualAppliance	1stOrgGroup	Critical	6 min.	--
win7-x86-EN	VirtualAppliance	1stOrgGroup : VirtualSite	Critical	--	
vm2000pro-en	VirtualAppliance	1stOrgGroup : 2000VoVSS	Warning	--	
vmsbs-2003-en	VirtualAppliance	1stOrgGroup : 2000VoVSS	Good	6 min.	--
VM-Win7x64-PC	VirtualAppliance	1stOrgGroup : VirtualSite	Good	6 min.	--
Win7-x64-De	VirtualAppliance	1stOrgGroup : VirtualSite	Good	6 min.	--

The Portal EndPoint list functions the same as the EndPoint list shown in the Main Panel on a single CMD appliance. However, the Portal list does include one additional column--the *Appliance* column--to identify the appliance monitoring this particular EndPoint.

Portal Session Panel

The Portal Session Panel appears at the top of the console:



This panel displays:

- | | |
|--------------------------|---|
| User | This identifies the name of the currently logged-in user. |
| Account Settings | Displays the currently logged-in user's settings in the Main panel. The user can then change their password, email address, or type of notifications to receive (All, Critical, or None). Click Save to save the new settings. (Use <i>Portal Accounts</i> to change the administrative role if needed.) |
| Help | Opens this <i>ShadowControl CMD User Guide</i> in a new tab in the browser. |
| Logout | Logs the user out of the portal console. |
| Portal Identifier | In the lower-right corner of the Portal Session panel is the word "Portal". This indicates that this console is a Portal (as opposed to an appliance) console. An appliance console would indicate the name of the appliance. Portals do not have names, as there can be only one portal per CMD system. |

8.2 Using Org Groups

Select *Org Groups* from the portal's Navigation panel to display a list of the defined Org Groups and options to add to or edit those Org Groups:

Org Groups - PhysicalApp

Org Groups are collections of Organizations from one or more appliances.

Org Group	Actions
MSP 1	

+ Add Org Group

Actions

You have three actions on the Org Group page:

Icon	Description	Function
	Blue pencil icon	Opens the selected Org Group's configuration page. Use this page to edit the selected Org Group's name, contacts, or status rules. (See Using Status Rules for more details.)
	Red delete icon	Deletes the selected Org Group.
Add Org Group button	Opens a Org Group configuration page. Specify the name and contact info for this new Org Group.	Note: Org Group names support multi-lingual characters.

Click **Organizations** in the Navigation panel to add organizations to a defined Org Group shown in the dropdown box:

Organizations

Assign the Organizations from the Appliances into Org Groups. Use the options in the Appliance views to create new Organizations.

Organization	Appliance	Org Group
1stOrgGroup	VirtualAppliance	MSP 1

8.3 Portal Report Scheduling

Select *Reports* in the Portal Navigation panel to display the Report Scheduling page in the Main panel:

Report Scheduling

Schedule the generation of reports tailored to specific administrators and contacts. Reports are sent by email according to the selected schedule.

SuperAdmin Report

Send a report to Appliance SuperAdmins for each appliance Send reports: **Never**

Report will contain a Summary section and any of the following sections:

EndPoint Status: overall status of all monitored EndPoints
 EndPoint Backup: listing of last backup for each ShadowProtect installation

Administrator Report

Send Appliance-level, organizational report to Administrators of each Appliance Send reports: **Never**

Report will contain a Summary section and any of the following sections:

EndPoint Status: overall status of all monitored EndPoints
 EndPoint Backup: listing of last backup for each ShadowProtect installation

Organization Report

Send an organization report to the primary contact of each organization on all appliances Send reports: **Never**

Report will contain a Summary section and any of the following sections:

EndPoint Status: overall status of all monitored EndPoints
 EndPoint Backup: listing of last backup for each ShadowProtect installation

[Copy Schedule to Appliances](#)

These report scheduling settings are similar to the [Appliance Reports](#) settings for a CMD appliance with these exceptions:

- These portal report settings are sent to each of the appliances. These settings will then supercede any existing settings on the appliances for the associated reports. The individual appliance's SuperAdmin or administrators can, however, adjust these settings on their individual appliances as needed afterwards.)
- These settings apply globally to all reports for the affected organizations, appliances, or SuperAdmins.
- These settings are not stored at the portal level. Instead, they are copied down to and stored at the affected appliances.

8.4 Defining Portal Accounts and Settings

This section covers:

- Portal Accounts
- Portal Settings

Portal Accounts

The *Portal Accounts* option in the Navigation panel acts the same as the [Appliance Accounts](#) option on an individual appliance. Use this option to specify SuperAdmins, administrators, and read-only access for this portal. The difference is that an administrator or read-only account on the portal can be assigned to organizations from *multiple*, rather than just *one*, appliance.

Portal Settings

Select this Navigation panel option to display the portal settings in the Main panel:

tom-int-appl02

System Info

Version: ShadowControl v1.3.0.29138 [1.7-29138, 45] [Release Notes](#) [Update Appliance](#)

Access Code: func0

RAM Usage: 540 MB of 995 MB available (45.7% used)

Disk Usage: 12 GB of 14 GB available (14.3% used)

CPU Usage: 0.00

Load Average (5 min.): 0.42

Appliance Timezone: America/Cuiaba
 America/Curacao
 America/Denmarkshavn
 America/Dawson
 America/Dawson_Creek
America/Denver

[Set Timezone](#)

[Reboot Appliance](#) [Shut Down Appliance](#)

Appliance Backup

Email Settings

Network Settings

Security

Product Registration

These sections appear, and the settings function, the same as for the [Appliance Settings](#) on a single CMD appliance. The difference

is the lack of a subscription section at the bottom, as a portal cannot subscribe to another portal or appliance.

9 Appendix: Experimental Report API

ShadowControl CMD includes two experimental reporting APIs for use by developers to access EndPoint information:

- Historical EndPoint Data
- Current EndPoint Status

The results are sorted by organization then by site. Each API filters these results based on the credentials entered. Superadmin credentials deliver complete data, while lesser credentials deliver data for only those EndPoints the user is authorized to monitor.

Historical Data Reporting: /api/reports/history/[<endpt uuid>/]

```
{
  "<endpt uuid>": [
    {
      "name": "<endpt name>",
      "org": "<current org <org>[:<site>]",  

      "timezone": "<endpoint's timezone given as seconds offset from UTC - only given if available>,  

      "summary": [
        {
          "ts": "<date of info for day 1>",
          "jobs_successful": "<number of successful jobs completed on this day>,  

          "jobs_aborted": "<number of aborted jobs>,  

          "jobs_failed": "<number of failed jobs>,  

          "img_total": "<number of backup images saved during the day>,  

          "total_size": "<total size of all backup images in Bytes>,
        },
        "...for day 2",
        ...
      ],
      ...
    },
    ... (one entry for every endpt in the request)
  ]
}
```

Current Endpoint Status Reporting: /api/reports/status/[<endpt uuid>/]

```
{
  "<endpt uuid>": [
    {
      "name": "<endpt name>",
      "org": "<org>[:<site>]",  

      "timezone": "<endpoint's timezone given as seconds offset from UTC - only given if available>,  

      "status": "<current endpoint status: ok, warning (yellow), critical (red), offline(=endpoint not responding)>,  

      "lost_contact": "<minutes since appliance's last contact with the endpt, 0 if endpt is currently responding>  

      "shadowprotect": {
        "jobs": [
          {
            "name": "<name of job1>",
            "policy": "<name of ShadowControl policy used to create the job, omitted if no policy>  

            "status": "<current job status; queued, pauses, etc.>",
            "next_run": "<datetime of next scheduled backup>",
            "last_run": "<datetime of last backup>",
            "last_mode": "<type of last backup; full, incremental>",
            "last_result": "<result of last backup; success, failure>",
            "last_success": "<datetime of last successful backup>",
            "destination": "<path to destination>"
          },
          {
            "name": "<name of job2>",
            ...
          },
          ...
        ],
        ...
      }
    }
  ]
}
```

```

},
"imagemanager": {
  "folders": [
    {
      "path": "<path to folder1>",
      "state": "<current state: active = 10, syncing = 20, offline = 30, failure = 40>",
      "file_count": "<number of files in folder>",
      "folder_used_mb": "<total folder size in MB>",
      "vol_total_mb": "<filesystem total size in MB>",
      "vol_free_mb": "<filesystem free space in MB>",
      "consolidation_errors": [
        {
          "code": "<error code, reserved for future use. currently empty>",
          "details": "<error as produced for display in IM>",
          "ts": "<datetime of failure>",
          "filename": "<name of the file that failed during consolidation>",
          "volume": "<volume name>",
        },
        ...
      ],
      "verify_errors": [
        {
          "code": "<error code, reserved for future use. currently empty>",
          "details": "<error as produced for display in IM>",
          "ts": "<datetime of failure>",
          "last_success": "<datetime fo last successful verification>",
          "volume": "<volume name>",
          "collapse": "<type of collapse attempted>",
          "snap_ts": "<datetime of snapshot>",
          "chain": "<UUID of chain (can be used in IM Rest API to access more chain info)>",
          "file_size": "<file size (in MB)>",
        },
        ...
      ],
      "replication": [
        {
          "name": "<replication job name>",
          "status": <IM's description of current status>
          "queued_files": <number of file waiting to be replicated>
        }
      ],
      "hsr": [
        {
          "uuid": "<uuid of hsr job>",
          "name": "<hsr name>",
          "state": "<summary state>",
          "jobs": [
            {
              "uuid": "<uuid of hsr target>",
              "path": "<path of hsr target>",
              "state": <target state>,
              "status": "<string displayed by IM describing target's current status>",
              "last_update": "<datetime of last HSR update for this target>",
            },
            ...
          ]
        }
      ],
      ...
    },
    ...
  ],
  ...
}
... (one entry for every endpt in the request) }

```